McNAIR PAPER 61

Illuminating Tomorrow's War

Martin C. Libicki

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 1999	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Illuminating Tomorrow's War	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Martin C. /Libicki	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
National Defense University Institute for National Strategic Studies Fort McNair Washington, DC 20319	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

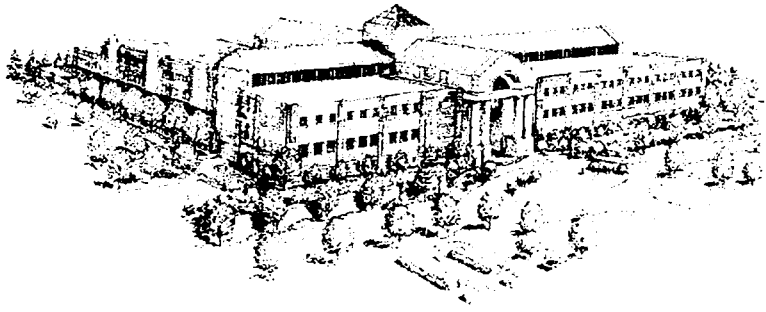
14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**140**	

The Institute for National Strategic Studies (INSS) is a major component of the National Defense University (NDU), which operates under the supervision of the President of NDU. It conducts strategic studies for the Secretary of Defense, Chairman of the Joint Chiefs of Staff, and unified commanders in chief; supports national strategic components of NDU academic programs; and provides outreach to other governmental agencies and the broader national security community.

The Publication Directorate of INSS publishes books, monographs, reports, and occasional papers on national security strategy, defense policy, and national military strategy through NDU Press that reflect the output of NDU research and academic programs. In addition, it produces the INSS Strategic Assessment *and other work approved by the President of NDU, as well as* Joint Force Quarterly, *a professional military journal published for the Chairman.*



George C. Marshall Hall

Illuminating Tomorrow's War

Martin C. Libicki

McNair Paper 61
October 1999

INSTITUTE FOR NATIONAL STRATEGIC STUDIES
NATIONAL DEFENSE UNIVERSITY
Washington, DC

National Defense University
ATTN: NDU-NSS-PD
300 Fifth Avenue (Bldg. 62)
Fort Lesley J. McNair
Washington, DC 20319–5066

Telephone: (202) 685-4210
Facsimile: (202) 685-4806

For sale by the U.S. Government Printing Office
Superintendent of Documents,
Mail Stop: SSOP,
Washington, DC 20402-9328

ISSN 1071-7552

Contents

Acknowledgments

The author gratefully acknowledges the very kind help of the following people who provided information for or reviewed and commented on previous versions of this report.

David Alberts
Kirstie Bellman
Alvin Bernstein
James Blaker
Richard Casey
Patrick Cronin
Bruce Deal
John Evanoff
Jerry Faber
Edward Feighenbaum
Howard Frank
Frederick Giessler
Jeffrey Gerold
Seymour Goodman
James Graham
Mary Hammond
Delonnie Henry
Ryan Henry
Sam Hubbard
Jeremy Kaplan
Michael Martus
Ray Michael
Ronald Montaperto
Lindy Moran
Anthony Oettinger
John Reed
George Ruptier
Ellin Sarot
Alan Sears
Howard Shrobe
Jerry Smith
Shukri Wakid
Tom Welch

Prologue

> [The] information revolution is creating a Revolution in Military Affairs that will fundamentally change the way U.S. forces fight . . . [supported by a] "system of systems" that will give [United States forces] superior battlespace awareness.[1]

In the weeks leading up to *Desert Storm*, anxious analysts tried to forecast the course of war by counting what the coalition and Iraq each brought to the battlefield: they have this many men, we have that many men; they have this much armor, we have that much armor; their air fleet is this big; ours is that big. Few doubted which side would prevail in battle, but many analysts were not so sure the war could be won swiftly and with acceptable casualties.

Looking back, their worries seem baseless and their correlation of force calculations almost quaint. Indeed, the coalition may have carried the day almost as well with only half the forces. By the time the planes came back from Baghdad, Iraq was blind, but the coalition could see. That, plus precision weapons (and people trained to use them) determined the outcome. All else was detail.[2]

The Gulf War suggested that the ability to see the battlespace is key to prevailing in conventional conflict when technology permits forces to hit and kill what they can see. This close relationship between seeing and striking may affect everything about conventional warfare: how it is fought, what forces and equipment it is fought with, and the role of the United States and others in fighting it.

To illuminate the battlespace, the Department of Defense (DOD) uses sensors (to yield ISR: intelligence surveillance, and reconnaissance) and networks (to support C^4: command, control, communications, and computers). With precision weapons added, they collectively make up a "System of Systems."[3] Indeed, DOD *is* a System of Systems: its people deploy sensors, examine returns, maintain databases, create reports and maps, respond to orders and assignments, and designate targets for weapons. Rising complexity, a growing aversion to risk, the need for speed, constant cost pressures, and technological opportunities[4] all impel automatic integration of components at all levels from bits to knowledge. Otherwise, the vision of the battlespace remains a patchwork.

Integration offers the possibility of creating what has been called a Global Grid, referred to in this volume as the Grid.[5] It would be the glue of the "System of Systems," the means by which systems are linked and accessed, and a knowledge base—at a minimum, the common operational picture (COP)—built over and by a network. The Grid would "know" things in the sense that information (1) existed in some database,[6] (2) could be retrieved by content, and (3) was internally consistent across the Grid. Users on the Grid could be electronically connected to other warfighters and collaborate with them, can see a real-time map of the battlefield, annotate this map for others, find out where parts are in their repair cycle, participate in a simulation or exercise, assess the state of the network (and perhaps defend it from attack), diagnose remote equipment, and even perhaps call for fire support from certain weapons. Indeed, being continuously and intimately connected to the Grid may be second nature for tomorrow's forces.

This monograph explores some implications of and requirements for achieving battlespace illumination. Laced through this monograph are several themes: the ascendancy of light over power in arbitrating conflict, the sunset of platform-centric warfare in favor of Grid-centric warfare based on distributed sensors and weapons, the tension between the war that we would fight (e.g., standoff warfare) and the war our enemies may prefer, the need for a good mix between mission-oriented and user-oriented applications, and the need to keep the Grid open to change, and perhaps opened to others.

Those familiar with the debate over the revolution in military affairs (RMA) may find concepts in chapters 1 through 3 familiar,[7] and those thinking about information systems may respond similarly to chapters 4 and 5. Consolidating these strands of thought (and adding a few others) may broaden both the readership and the discussion of these issues.

Illuminating Tomorrow's War

1. Foundations

> [The United States is] converging very rapidly . . . to see all high-value targets on the battlefield at any time . . . to make a direct hit on any target we can see, and . . . to destroy any target we can hit . . . to make the battlefield untenable for most modern forces.[8]
>
> *Under Secretary of Defense William J. Perry* (1978)

The United States is midway through what may be called a revolution in military affairs (RMA).[9] This revolution opened in the 1970s with the development and refinement of precision-guided munitions[10] (PGMs), which can hit anything that can be located. It is likely to culminate with the multiplication and integration of the DOD C⁴ISR assets, thereby creating a well-populated Grid. In the process, the physical battlespace will become illuminated better than ever. As this occurs, conventional warfare will change from force on force to hide-and-seek. Hence the need for a Grid capable of illuminating the battlespace, a case that rests on five tenets:

- With precision weaponry, seeing a target is tantamount to being able to kill it. The guidance for such weaponry is

potentially shifting from shooters or internal sensors to externally provided information.

- Defenses exist against PGMs, but the link between seeing and hitting is likely to strengthen over time.
- Detailed earth mapping and global positioning systems (GPS) have become important elements in locating targets. Access to GPS can be defended and can also be denied to adversaries.
- The growing power and variety of sensors mean things will be easier to see, data fusion (in the Grid) will become more important, and an architecture of distributed sensors may perform better (and survive longer) than one that concentrates on a few expensive sensors.
- The underlying technology, however, is available to all, which means the shift from force-on-force warfare to hide-and-seek conflict is not just a possibility, but a necessity.

Precision-Guided Munitions

Before the development of PGMs (especially long-range PGMs), knowing what was where was helpful, but such information was only one step toward defeating adversaries. Waging war required massing shooters and ordnance, coordinating platforms and their support, putting them in harm's way, and getting them to work right in the fog and friction of war.

Precision weapons promise greater effect (missed shots tell adversaries to hide, flee, or shoot back) from fewer shots, as well as fewer unwanted side-effects (such as hitting the innocent). As precision weapons increase the probability of destroying what can be found and tracked, so military outcomes are becoming a matter of who can see (and how quickly) and who can hide. Knowing what's where is primary and raw firepower secondary. Whether complex, expensive platforms are the best way to illuminate the battlespace and get firepower on revealed targets is not clear. What is clear is that platforms are far more visible and costly than the munitions required to destroy them (even if fired as clusters in a saturation attack) or the sensors required to find them.[11]

A target can be found if its general location is known and its movement can be tracked either manually or automatically (which

means, these days, electronically). It can also be found if its precise location can be ascertained in real time and conveyed to a weapon. PGMs can be classified accordingly: man-guided, seeker-guided, or point-guided.

Man-guided PGMs include the tube-launched, optically tracked, wire-guided missile (TOW) and fiber-optic-guided antiarmor missiles (FOG M), as well as those steered indirectly by laser. These PGMs tend to be cheap but do not fly far (the targeter needs to see the target). Targeters (such as those who hold the laser beam on the target) may be attacked; even if they survive, they may take their eyes or beams off the target and thereby break a lock. Given this limitation, these PGMs offer only a modest advantage over very accurate conventional direct-fire weapons (such as an M-1 tank, which can hit a target at 3,000 meters).[12]

Seeker-guided PGMs home in on a target's signature. Examples include PGMs that are heat seeking (the Sidewinder and Stinger short-range antiaircraft missiles and the infrared Maverick), acoustic (torpedoes), and radar-guided (against aircraft and ships). Newer kinds would recognize a target as an infrared (IR) image in a focal-plane array by using light detection and ranging (LIDAR). Future PGMs will use a combination of signatures (the Brilliant Antitank submunition weapon, for example, looks for both heat and sound). The more elaborate the guidance package, the more expensive the PGM, and a single missile in this class usually costs between $100,000 and $1,000,000.

Point-guided PGMs include ballistic missiles that use inertial navigational systems (INS) to determine where they are in real space; cruise missiles that fly according to internal maps; and new munitions that supplement INS[13] with GPS updates. These last can be inexpensive; one type, the Joint Direct Attack Munition (JDAM) costs $14,000 per kit[14] (compared with the planning estimate of $60,000).

Today's point-guided PGMs are trained on immobile points, but tomorrow's might use real-time updates to home in on moving targets (if the time required to get data from a sensor, through the Grid, and to the PGM is short enough for the missile to outmaneuver the target).[15] They justify building a real-time tableau of the battlespace from which PGMs draw their aimpoints.

PGMs that supply their own guidance must contain long-range sensors, but their cost makes them expensive, and high costs lead to small production runs (thus yet higher costs). Each sensor package is often tailored to a specific type of target. Point-guided PGMs are vulnerable to disruptions in GPS signals and communications that link sensors, navigation aids, and the PGM. But guidance can be generated by fusing the data from a large population of sensors, many times more capable than what a PGM can carry. The more powerful the sensing, the more easily a PGM can find and lock onto a target whose signatures are intermittent and ambiguous. Rather than being diverted to the last known location of the target, the PGM can follow predicted tracks. Because point-guided PGMs will not need to carry complex sensors, they will be cheaper and can therefore be bought in larger numbers. Attacks by volleys of PGMs can succeed by saturating a target's defenses.

If the DOD favors seeker-guided PGMs, it will have less need of (and less money to spend on) very sophisticated C^4ISR systems that provide external targeting. Favoring point-guided PGMs would require building such systems. Supplying only point-guided PGMs to temporary friends (such as Afghan mujahideen) limits the mischief such friends can do on their own after U.S. support ends.

In practice, external sensors could be used to localize a target. The PGM flies to a given point, and then uses its own sensors for terminal guidance. Such short-range sensors need not be so sensitive as long-range sensors and thus may cost far less. Alternatively, a local unmanned aerial vehicle (UAV), carrying more or better sensors than the PGM, can lase the target for the munition.

A target that has been detected may still try to escape destruction by spoofing, exploiting range or armor, or counterattacking. Despite these defenses, the odds still favor PGMs. Spoofing includes the ejection of flares (used against IR missiles), chaff and jammers (against radar missiles), and off-board sound generators (against acoustic PGMs, such as torpedoes). The efficiency of such defenses depends on the quality of warning systems potential targets carry. Although spoofing technology continues to advance, given the growing variety of signals a PGM can use for homing, the likelihood that a PGM will find its way is increasing. A PGM with an aimpoint determined by

fusing information from many external sensors would be harder to spoof than a PGM that has to rely on the one or two sensors it carries.

Targets are sometimes hard to hit even if they can be tracked. Aircraft such as the Airborne Warning and Control System (AWACS) and the Joint Surveillance Target Attack Radar System (JSTARS) operate beyond the range of most missiles today. With enough head start, some targets (one example being submarines) may outrun the PGM long enough for its fuel to be used up; others may outmaneuver the PGM. Future PGMs will fly farther and faster, so ultimately, the cost of making platforms faster or more agile is higher than that of improving PGMs.[16]

Armor will improve, but barring a breakthrough in materials, armor is no guarantee and adds cost and weight. Both Russia and the United States are working on a tank that collects information (speed, bearing, type) on an incoming round and, in response, reshapes its skin to a geometry that can blunt the impact of a missile, but such skins will be vulnerable to heavy weapons, fast penetrators, and saturation attacks. Like armor, burial provides a primitive but effective technology for command posts and high-value stores, but it cannot protect assets that must move. Meanwhile, bunker-busting bombs are getting better at penetration.

Shooting back is an option. The Army is working on lasers that can blind IR missiles, and the Navy on antitorpedo torpedoes, but both remain to be fully tested, particularly against swarm engagements. DOD has spent billions to learn how to shoot down Scuds, but so far results are mixed.[17] The Patriot missile was less successful in the Gulf War than initially believed. Upgrades and new missiles seem impressive in one-on-one test engagements, but they are not proof against saturation attacks.[18] Meanwhile, PGMs are becoming stealthier. European missile manufacturers reportedly are applying radar-reducing finishes to tactical missiles (such as the Penguin or the FOG-M).

Electromagnetic pulses or microwave bursts could be used to cripple the electronics on incoming missiles (although it is hard to time the burst just as the missile comes into range). Switching to PGMs with older technologies (such as mechanical fuses or terminal

trajectories) could nullify such electronic weapons but large-scale fuse replacement would be costly.

Defenses against PGMs have considerable life left in them. U.S. defenses against PGMs in the inventories of Third World countries would probably work better than Third World defenses against U.S. PGMs, but time favors the PGM. A valuable target would be difficult to defend against a swarm of stealthy missiles.

Precision Location

Many PGMs can track and hit targets without knowing the absolute location of either. Yet, absolute location lets PGMs get their guidance from a real-time map built by fusing a wide variety of external sensors. Precise mapping allows a target that lacks a real-time signature to be hit. Some perfectly camouflaged structures may be discovered by looking for elevation differences between a newly taken picture and baseline three-dimensional imagery of an area.

Absolute location requires good maps of the battlefield, which are being improved to multimeter level accuracy (Digital Terrain Elevation Data Level 4+ capability), thanks to satellites with electro-optimal imaging and interferometric synthetic aperture radar (SAR).

GPS, though, is the key to exploiting maps. Originally designed for guiding nuclear missiles, it proved itself for tactical purposes by permitting coalition forces to carry out complex maneuvers on a featureless terrain. Saddam Hussein was so confident that U.S. forces could not operate in trackless desert that he set up few defenses against the coalition's Left Hook attack, which outflanked his forces on the west.

GPS is now being used to guide U.S. tactical missiles. Unfortunately, it can also guide missiles of others. By 2010, Syria, Iran, India, and China may all have hard-to-see missiles guided by a combination of GPS and inertial navigation.[19] The trick is to deny GPS to enemies, retain it for friends, and minimize the impact on global transportation systems grown dependent on it. Originally, designers thought that the signal available to the public, accurate only to a 100 meters, was not good enough to guide enemy missiles. Only the military signal, accurate to within 18 meters, was. Then differential GPS (DGPS) was invented in early 1990s. Broadcasting

corrections between the GPS-measured location of a reference receiver and its true location[20] cut error to a few meters. Such systems are being installed throughout the United States, Europe, coastal China, and Japan.

Thus other methods must be used to deny GPS. The accuracy of GPS readings can be degraded by having satellites distort their own signals, but this could corrupt readings for every point visible from each satellite (a third of the earth's surface). Such distortion does not defeat DGPS but requires only that corrections be broadcast more frequently (every few seconds rather than every minute).

Another way to limit an adversary's use of GPS is to jam the public signal locally. Under the best conditions, a 1-watt jammer can incapacitate a civil GPS receiver within 20 kilometers. U.S. forces could pick up the encrypted military signal (broadcast on jam-resistant spread spectrum) using military equipment[21] with sophisticated antennas (that focus on where individual GPS satellites are[22]) and nulling devices (that block signals coming from other locations). The combination would be a million to a billion times harder to jam than a public signal acquired by commercial equipment. But access to the public signal is necessary to calibrate timing so that the military signal can be picked up; if gone, units may need to access precise clocks, which cost several thousands of dollars each. Jamming can also be defeated by using accurately placed pseudo-lites (that use spread spectrum or frequency-hopping to get through) to substitute for GPS signals.

All in all, GPS is valuable, but access to its signals must be carefully managed. U.S. forces will have to find ways to deny the public signal to enemies and still exploit the military one.

A World of Sensors

The ability to destroy any object that can be located or that has a trackable signature establishes the value of seeing the battlespace (without being seen). Sensors—which range from cameras and microphones to radar, passive receivers, and biochemical detectors—are the foundation for illumination because they can be placed in harm's way, can be used flexibly,[23] and create digital information that can be transmitted, manipulated, and fused.

With integrated circuits, laser emitters, and detectors growing cheaper by the year, sensors grow increasingly cost effective. What talks emits electromagnetic signals. What moves reflects doppler and disturbs the environment. What is solid stands out from water, air, or vacuum. What uses energy gives off heat. What stands still can be found through painstaking search. The more bits collected from the environment, the finer the weave that can be thrown over the battlespace. Eventually, what can be sensed, will be.

As a result, the United States can enjoy growing confidence in its ability to see opposing forces and their platforms. The burgeoning number and variety of sensors suggest the scope and value of data fusion, the wisdom of networking sensors rather than seeking some super sensor, and the joint nature of battlespace illumination.[24] Opportunities for shifting from stand-alone sensors to sensor Grids abound in all media.

Space-Based Sensors

Today's powerful space sensors were designed for strategic rather than operational purposes. Those that fly in low-earth orbit (LEO) take detailed pictures in the visible, IR, and microwave bands (including synthetic aperture radar, SAR, and inverse SAR). Coverage is discontinuous: enough for a few shots, then nothing until they return a few days later. Because LEO satellites travel in predictable orbits, an adversary can hide or halt activity while they are overhead. Geosynchronous satellites provide continuous observation of specific spots but operate at a distance of 36,000 kilometers and so have very low resolution. Generally, they are used for electronic intelligence, early warnings of missile launches (by IR detection), and meteorology.

Satellites that constantly look over a battlefield, even with lower resolution than today's surveillance satellites, could monitor movement, frustrate hiding when the satellite is overhead,[25] and thereby serve tactical purposes. The planned DOD space-based infrared satellite constellation would combine four geosynchronous satellites for broad surveillance with a constellation of LEO satellites for precision cuing and tracking. In early 1997, the Defense Advanced Research Projects Agency (DARPA) proposed Starlite (now called Discoverer 2), a constellation of 24 satellites flying at 700

kilometers that can collectively revisit any point within 15 minutes or less (13 more satellites would permit 8 minutes between visits); resolution would be 1 meter, give or take a factor of 3, depending on the choice between scan and spot mode.[26] The success of the Ballistic Missile Defense Organization's multiple-sensor technology integration (MSTI) satellite and Clementine spacecraft suggests that fleets of hundreds of inexpensive satellites ($30 million and $50 million, respectively, plus launch costs) could provide adequate resolution in LEO. Both MSTI and Clementine had multiple sensors (each weighing roughly a kilogram), some capable of imaging to 20 meters (one Clementine sensor could see down to a few meters). The National Aeronautics and Space Administration's (NASA) Clark satellite and planned private surveillance satellites (such as the one from CTA, Inc.) confirm that a $50 million satellite can take pictures that are accurate to 2 or 3 meters.[27]

Rapid dissemination of imagery to the field is crucial if militaries are to respond to transient data. In 1995, U.S. forces advanced toward receiving real-time data from French satellites. With this as a harbinger, military use of third-party satellites, even those configured for environmental purposes, is likely to rise substantially.

Airborne Sensors

JSTARS (which uses radar to track ground targets), AWACS (which monitors the air picture), Rivet Joint (which collects electronic intelligence), and Cobra Ball (which uses IR sensors to track missiles) aircraft all carry extremely capable sensors. Yet their airframes (Boeing 707s, RC-135s) are hardly stealthy, and both JSTARS and AWACS must emit energy to generate the echoes they read. As more countries acquire missiles of sufficient range, DOD will be required to replace such aircraft with constellations of UAVs, each with similar if less powerful sensors.

UAVs offer several advantages over satellites. They can loiter over a target and operate up to a hundred times closer to it, often under cloud cover. The same optical sensor package that yields a 10-meter resolution from space can yield a 0.3-meter resolution from 5 to 10 km high. They can identify objects that can only be spotted from space.

But because they violate airspace, UAVs can create political problems if caught in peacetime. Today's UAVs need many operators, some within range of the battlefield. If spotted, UAVs can be blinded by lasers or destroyed by gunfire or missiles. Smaller than aircraft, they can be stealthier, yet the mission of continuous observation requires they be used in daylight (which makes them more visible) as well as at night. Because most UAV communication is through imagery, it must use high-bandwidth channels, increasing the risk of detection (if enemy detectors stand between the UAV and the receiver—an argument for space-based relays).

DOD is developing several types of UAVs, many of them setting standards for performance of sensor packages, systems integration, range, loitering time, stealth—and cost. These include the Predator and the Gnat (relatively inexpensive and capable but vulnerable when flying under 1,200 meters), the Dark Star (a stealthy bird flying at 20 kilometers, capable of carrying payloads of several hundred kilograms), the Global Hawk (which can carry a ton of payload but costs more than $10 million), and tactical UAVs, such as the Outrider, the Hunter, and the Israeli-built Pioneer. A constellation of many, cheap, short-loiter UAVs may be useful when clouds are thick and SAR resolution is too poor to differentiate among potential targets. A UAV that can do useful chores but costs less than $5,000 apiece would be at least 10 times less expensive than the cheapest missile that could shoot it down.[28] Rotary-powered UAVs have been proposed for urban missions.

Tethered aerostats—modern-day dirigibles that float as high as 20 kilometers and can see air and ground targets as far away as 500 kilometers—can be used for early warning. One is already up over the Persian Gulf. Because, unlike UAVs, they do not have to be launched and recovered periodically, they should cost less to operate. Once shooting begins, however, their immobility makes them easy targets.

Ground-Based Sensors and Soldiers

Improved ground-based sensors[29] can supplement more familiar spectral sensors in finding targets. Densely placed microphones might prove valuable in finding aircraft (such as a B-1) or cruise missiles that fly below radar but leave a distinct trail of noise. Small cameras

(especially with night-vision capability) may keep critical junctions under surveillance.

Some ground-based sensors can detect traces of airborne phenomena such as pressure variations, vapors, and chemical emissions. Sniffers may detect motor emissions and even a human presence. Metal objects in motion may be detected because they disturb magnetic fields (much as stop lights are cued by the movement of vehicles). Gravimetric sensors differentiate among empty, lightly loaded, or densely packed trucks. Seismic or acoustic sensors can find otherwise undetectable underground structures or pick up the vibrations caused by the surface movement of large vehicles. Reliance on any single ground-based sensor for accurate identification is liable to result in missing much traffic and generating false alarms. Yet a combination of many ground-based sensors used with standoff sensors could improve overall detection.

The deployment doctrine of sensors varies with range and endurance (which are correlated attributes). Because short-range sensors provide wide-area coverage only if used in large numbers, they must be cheap. For adequate triangulation of signature sources, they must also be networked. Short-range sensors could be used as adjuncts to long-range sensors, for confirmation and to complicate an opponent's efforts to diminish its equipment's signatures. Temporary sensors (to monitor a possible event or sown over terrain liable to be disturbed) can be cheap battery hogs; quasi-permanent ones must be rugged energy-misers.

Tomorrow's soldiers, themselves intelligent mobile sensors, may go armed with devices 20 to 50 times more powerful than today's laptops, digital radio-based communications capable of exchanging video data, and electronic image-quality maps updated in near real time by UAVs and other sensors.

Naval Sensors

Shipboard sensors operating from international waters can pick up electronic signatures, listen to port operations, oversee the flight operations of coastal cities, peer into mountainous terrain, and from some locations, pick up radar signatures that hug the earth. But much that ships can sense requires they sail within 20 kilometers of a hostile

coast (and that close, a line-of-sight sensor must be 30 meters high to see anything on the water). At that range, ships may be seen by many land-based weapons.

Mine warfare adds risks in shallow waters. Although not widely reported, antiship mines caused more damage to coalition assets in the Gulf War than any of the more highly publicized systems. Future shallow-water mines (plastic mines, for example) will be harder to detect (if they resemble littoral clutter) and defeat (if they can be cued by external sensors).[30] Once fired, they could take on the characteristics of torpedoes, capable when used in concentration of sinking even the largest ships. Naval aircraft extend the effective range of ships, but carriers are few and expensive, and on peacetime rotation they average only 4 months a year on station (usually 2 to 3 months for remote sites such as the Indian Ocean).

A series of buoys, especially if complemented by ship-launched UAVs, may prove useful for collecting signatures. Buoys are individually less capable than ships but, in sufficient number, could offer a radar "dish" strong enough to simulate today's land-based, over-the-horizon backscatter radars. Distributed buoys would need to pass an enormous amount of data back and forth to form a coherent picture, presenting a challenge that computers of 2015 should be able to handle.

Using Sensors

The potential for communications among sensors is likely to influence the architecture of sensor Grids. Precision targeting ordinarily occurs in three steps. Sensors scan for a few interesting objects within a large area. Filters discard most data and leave selected patches for further machine or human analysis, then targets are pinpointed and tracked, often by other sensors so that they may be struck. The relationship between cuing and pinpointing sensors can be complex. A spacecraft that has surveyed a target area and detected phenomena that merit attention can ask a UAV to alter its search pattern. The UAV then takes a closer look and cues ground sensors to turn on acoustic and biochemical capabilities for confirmation. Or UAVs monitor ground sensors and react to the data they send.

Synoptic pinpointing—finding targets by surveying the entire battlefield at high resolution and shipping the bits to a single point for analysis—will not work except under certain conditions. A single image of the notional 150,000 kilometers^2 (200 nautical miles squared) battlefield at a 0.1-meter resolution (with 8 spectral bands at 8 bits of data each) constitutes a quadrillion bits of data that need to be transmitted—enough to overwhelm any reasonably large slice of spectrum. Even 10:1 image compression (more risks the loss of considerable detail) leaves 12 terabytes of data to be handled. Still, tiered sensing remains a compromise. U.S. automatic target-recognition systems are the best in the world, yet even they tend to find only what they are looking for only where they are programmed to look.

A Mesh of Sensors

A single sensor capable of finding and classifying targets on its own would be the most straightforward way to survey the battlespace.[31] In general, as a medium grows denser, the opportunities for hiding increase, and sensing thus grows harder (density also reduces the distance a ground-based weapon can see and fly without running into something). Oceans, deserts, plains, and farms are the easiest environment in which to sense objects. Dry mountains and chaparral offer modest difficulty; forests and jungles more; and intact cities probably present the greatest challenge. With greater density, maintaining adequate cover calls for more airborne sensors complemented by ground sensors. As hiding becomes more important, adversaries will increasingly resort to cover, concealment, deception, and masking themselves as civilians. Distinguishing targets from everything else will take advantage of differences in factors such as weight, magnetic flux, radio frequency (RF), and chemical emissions, even habits and tracks. A target capable of fooling one type of sensor may not fool others that rely on different principles.

A mesh of heterogeneous, abundant, and overlapping sensors offers other advantages that data fusion can exploit. An object spotted by one sensor may disappear; its reappearance to another sensor operating in the same or a different spectrum is the beginning of integrated target tracking. Distributed sensors permit tracking targets

where coverage of any one sensor is intermittent (in rough terrain, within cities). Precision targeting means both accurate location and unambiguous identification: an electro-optical sensor may do the first, but acoustic or other sensors may be necessary for confidence in the second. Sensors accurate in one dimension may be inaccurate in another; using several at once can pinpoint a source. Certain ambiguous formations may be detected only if they match a predetermined template; again, with more sensors, each relying on a variety of methods, the probability increases that indications will be correctly identified or rejected as targets. Many sensors can defeat single-dimension decoy and stealth strategies. Coupling many lasers and optical sensors, for instance, can weave a fabric of light paths so dense that even the stealthiest platform cannot avoid cutting a few and so revealing itself. As sensors proliferate and targets grow more complex, data fusion and robust connectivity become more important.

There is also safety in numbers. A blinding strategy that attacks a military's eyes fails if there are so many eyes that no strategy to locate and remove them can substantially affect what the Grid sees. The few really good eyes in the U.S. space inventory may be vulnerable to attack. A constellation built from small satellites can be replenished by launching them from small rockets lofted under the wings of aircraft that take off from thousands of locations. Clearing an area of ground sensors (by using densely placed barrages or even nuclear explosions) may temporarily blur what one can see of the battlespace, as can an attack on the communications between sensors and operational forces. Maintaining an overlapping combination of close-in and standoff sensors along with a robust capability to reseed areas with follow-on sensors can negate the long-term effects of that tactic.

Although the technology of cheap sensors is not new, the difficulty of managing so many items and fusing the data they produce used to discourage their use. Correlating the readings of separated emitters and sensors (such as bistatic radars and laser-sensor grids) is particularly difficult. Sufficiently powerful computers can solve both problems.

What Will Be Visible?

Within a decade or two, U.S. forces should be able to detect reliably the presence, movement, and sometimes type of large platforms in tomorrow's battlespace—ships,[32] wide-bodied aircraft, and tanks and armored personnel carriers (unless well concealed)—and to determine the location and rough identification of military events, such as small platform movements, missile firings, artillery rounds, even some gunfire in real time and with enough accuracy for counterfire.[33]

Most forms of stealth probably will not work against U.S. sensor systems (except perhaps stealthy missiles over a short trajectory).[34] Yet passive sensors and weapons silently awaiting a signal before activation will be hard to detect, particularly if sufficiently small or indistinguishable from background objects and if not concentrated in expected locations. And as soldiers and their equipment look more civilian, differentiating between them from afar becomes harder.

The transparency of the battlefield a decade or two hence should be far greater than during the Gulf War (even with 6 months' preparation and in open terrain). Just before ground combat began, U.S. forces were able to identify, locate, and destroy almost all relevant conventional infrastructure targets (although it was not possible to know which housed WMD facilities), including major emitters, and roughly one-third of the tanks and artillery pieces. Despite the resources dedicated to hunting Scuds (at one point a third of the total F-15 fleet), no mobile launchers were sighted well enough to be confirmed as destroyed. Better tactical intelligence (and constant surveillance by UAVs may be key) may increase real-time sightings of Scuds[35] greatly (unless and until they start to look like regular trucks), moving targets considerably, and stationary targets only modestly.

The Potential Proliferation of the Revolution in Military Affairs

Today's PGMs and tomorrow's sensor networks are reasons enough for the DOD to shift from force-on-force to hide and-seek warfare. But as the sophistication of U.S. forces increases, so, too, will that of potential enemies. The capability for hide-and-seek warfare will not be an option but an imperative.

Militaries often refight their last successful war, and for the U.S. military the Gulf War was successful as few wars have been. The experience has provided U.S. force planners with their canonical foe—a middleweight rogue nation. This choice colors how and with what equipment DOD plans to fight. Iraq seemed not to appreciate the effects of modern information technology.[36] The assumption that the United States will again face an equally clueless adversary may prove costly.

The global electronics bazaar[37] may supply most components for a decent C^{4}ISR system: computers, communications, GPS receivers (which already fit into pocket pagers), satellite receivers, and cryptographic software, all of which get less expensive every year. By 2005, digital video disks, introduced in 1997, may hold 17 gigabytes—enough for a compressed color image of the Korean peninsula accurate to a meter. The sophisticated know-how—for installing and maintaining local area networks (LANs), high-speed switches, such as asynchronous transfer mode (ATM), computer operating systems (Unix or Linux), cellular telephones that resist jamming (thanks to spread spectrum), and videoconferencing equipment—is available everywhere in the world. Most potential Third World foes can field an information system comparable to one in a modern U.S. office building—maybe better in some respects than one in a typical U.S. command center (even if hardened against the hazards of war). DOD has equipment individually better than what is available in the open market but, by this point, not much better and a good deal more expensive.

Even sensors are commercially available. Digital video cameras mounted on UAVs—and more than 20 countries can make UAVs and 30 more may own some—may be a great source of battlefield pictures and video.[38] The resolution of today's consumer cameras, at roughly 500 lines, is imprecise, but high-definition digital television may create a market for high-resolution cameras with almost double the line density. Digital still cameras are already widely available.[39] IR detectors are common in home and office security systems, and personal radar devices,[40] laser pointers and rangefinders, and night-vision goggles are or soon will be commercially available.

As communications thicken worldwide, the likelihood drops that any military activity might occur unnoticed. The daylight movement of an infantry platoon past a village unconnected to the rest of the world could still be a secret today, but if and when that village were wired into the global telecommunications system, military movements could be reported as they occur. Mexico's *Zapatistas* have shown that even an irregular force on the run can have a Web presence. Range-finders, digital cameras, GPS, and cellular telephony combine into a handy, do-it-yourself targeting system,[41] add Web access, and such military movements can be communicated to the world.

Finally, a vigorous international market in PGMs exists, fueled by formerly Russian equipment, newly manufactured European devices, and leftovers from U.S. stockpiles. Of course, being able to buy the parts is not the same as being able to put them together. U.S. capabilities in the field of systems integration are unmatched, but many so-called underdeveloped countries have huge pools of technical talent: mathematicians from Eastern Europe, Ph.Ds from South Korea, electronics engineers from Malaysia, aircraft designers in Brazil and Indonesia, and millions of technically trained workers in China and India. Ultimately, any public information about technology will be available to anyone with an Internet link. Countries can also buy turnkey integrated systems such as highly sophisticated process-control machinery or air-traffic control systems (similar in many respects to military command-and-control systems). Deliberate technology transfer, maintenance experience, and reverse engineering may allow others to discover the essential techniques of systems integration.

The Proliferation of Space Capabilities

The United States is likely to enjoy superior access to space for decades to come. But others will use space in ways that make U.S. forces more visible.

Supplementing GPS, Russia's global navigation satellite system (GLONASS) came on line in 1995, and navigation signal add-ons are being mulled for other communication constellations. Europe may even launch its own fleet.

Overhead surveillance with 1-meter resolution can help find specific facilities. During the Cold War, only the Soviet and U.S. systems could see that well; now China expects to launch a 1.5-meter capability soon. Since 1991, a vigorous market has developed in Russian 2- to 3-meter imagery; with that and the projected launch of U.S. 1-meter imagery satellites, considerable real-time intelligence is for sale.[42] The advantages that U.S. imagery gave coalition forces in the Gulf War prompted many countries to consider obtaining better surveillance satellites, in particular France[43] and Japan (the latter ostensibly to monitor natural disasters). Exporting such satellites has enabled many countries to buy and transmit imagery in nearly real time.[44] Japanese satellites, using SAR, already resolve to 3 meters, and an Indian satellite can resolve to 6 meters using panchromatic sensors. The coupling of GPS, sufficiently good surveillance data, and long range PGMs could put almost every fixed facility at risk.

Third World nations can expect easier access to space. Many already own and run geosynchronous communications satellites. Early in the next century, television from direct broadcast satellites (DBS) may become ubiquitous in most of the world; military command-and-control signals could ride piggyback on some commercial channel. Because broadcasts of DBS satellites can reach several countries at the same time, jamming any one channel might be infeasible.

The increasing popularity of commercial space applications may limit what the United States can do to deny an enemy access to space. In the Gulf War, agreement with Russia was enough to protect the U.S. Left Hook maneuver into Iraq from being reported to Baghdad. As satellites proliferate, maintaining embargoes will be more difficult, perhaps impossible. Future foes may not be the pariahs Iraq was. Similarly, unless the owner of every communications satellite transponder—and there are more than a thousand within sight of any point on the globe—puts embargoes on the foes of the United States, transmission is inevitable. The United States could demand proof that the owners of all space systems are cooperating and could disable satellites of any that refuse, but would it be willing to enforce this rule short of global war? There are similar problems with jamming: it denies service to neutrals. Jamming a satellite in

geosynchronous orbit requires putting assets directly between it and its receiver platforms. Jamming radio communications that support guerrillas could interfere with the economic nervous system of a country that uses the same airwaves. And interference with the command and control of enemy aircraft could complicate regional attempts to monitor and regulate commercial air traffic.

What to Look For

Military intelligence assesses the progress of other countries toward the RMA by examining their doctrine as well as their current and in-the-pipeline equipment, most of it acquired and developed by established methods. Were these assessments reliable, other countries' RMAs could be seen coming years away, and the U.S. lead would remain intact. Given that RMA technologies are largely civilian, might RMAs be generated outside military organizations instead? A very effective military can be built from rummaging through the global electronic bazaars, something Third World strategists—military or not—can figure out. A large chunk of the RMA consists of superior intelligence and understanding of the control and use of land and immediate airspace. Dominating the battlespace can be seen as similar to other tasks of national space management, such as internal security, transportation management, urban and regional planning, even public health. Defense firms eager for customers may generate some notions of an RMA. Although these firms may not sell to rogue states, today's permitted customer may turn into tomorrow's enemy (as did Iran in the late 1970s). The tendency of U.S. intelligence to view standing armies and their equipment as indicators of military strength may be confounded by Third World strategists, who can develop new techniques for C^4ISR and other aspects of warfighting that will not show up in normal defense acquisition channels.

A civilian-based RMA would also confound the acquisition of templates. Battlespace knowledge is, to a large extent, about finding weapons of war (or their supporting infrastructure). If the weapons cannot be clearly seen, the next best approach is to build templates of emanations produced by weapons—sight, sound, smell, spectrum use—to generate probable identifications. This method works only

with knowledge of the weapons and of the patterns of their use.[45] Those monitoring Germany's use of tanks and radios to generate the blitzkrieg had the advantage of knowing what was being used, even if they did not know how it was to be used. A revolution that starts in a flash of insight may not comfort those looking for competing RMAs. Civilian-based equipment, organizations, and operational templates all may differ from what the United States traditionally expects.

Replaying the Gulf War

To illustrate what facing a more sophisticated foe can mean, consider the Gulf War as if fought in 2015. The United States did three things to win in 1991: it shipped in an enormous quantity of material, cut Iraq's ability to talk, and ran free over the battlefield, first in bombers, then in tanks. Circumstances will not favor repetition.

To fight overseas, the United States must lift forces there. Adequacy of the lift aside, would those forces survive the ride? Most countries now understand that Iraq was mistaken in allowing the United States to deploy unimpeded for 5 months, and future foes would probably contest such mobilization, making the littoral more hazardous. Surface ships are almost impossible to hide against most Third World and third-party surveillance assets. Very smart mines and torpedoes and saturation type cruise or ballistic missile attacks will be able to destroy ships within 200 kilometers of shore. Fast aircraft will be more elusive than slow ships but will not be able either to take many hits or to carry much on each trip. Ports and airfields also are vulnerable. The survival of logistics and command centers may require distributing their functions among subcenters and combining distribution with an agile information regime (to track supplies and messages, for example) as compensation for the effects of dispersion. If U.S. forces could be spread out widely enough, they might ride out WMD attacks, unless this strategy were obviated by geography—passes, isthmuses, valleys, and islands.

As communications options increase, cutting talk becomes harder. A wireline system can be disabled by bombing central office switches. A distributed wireless system may be less vulnerable, particularly if the size of circuitry were reduced so it could be carried on trucks or in briefcases.[46] Cellular systems leak telltale signatures, but useful

countermeasures include controlling unwanted sidebands, placing transmitters in dense, echo-laden environments (as Aideed did in Somalia), stringing wires out to expendable transmitters, and scattering emitting decoys. A foe could weave encrypted signals into a third-party live feed (such as Third World clones of the Cable News Network or could use third-party accounts on tomorrow's communications satellites (Globalstar, for example). Compression might be used to shrink the volume of message traffic; with many transmissions, at least one copy of every high-priority message might get through. Although communications systems can be attacked by knocking out power, if alternative power sources (fuel cells or photovoltaic power from holographic films, among other possibilities) become sufficiently inexpensive (maybe 6 cents per kilowatt hour), future power Grids may be built from sources too dispersed to target.

Maneuver has advantages: moving forces are more difficult to hit than immobile forces, can occupy superior firing positions, and by showing up where least expected, can disorient opponents and fragment their plans. Can these advantages persist against a foe armed with a deeply redundant sensor background and long-range precision weaponry? First, movement generates a larger signature than sitting still, and few moving platforms can outrun precision weaponry. Rather than break the lock that a shooter has on a target, movement creates disturbances—in earth, air, water, and spectrum—that confirm the lock. Second, range may cease to be a reason to move. A mesh of sensors controlled from afar may provide sufficient illumination, and medium-range PGMs (20 to 200 kilometers) may prove cost-effective ways for engaging most ground targets. Third, even though the shock of a massed attack can panic people, silicon, if intact, is not disoriented by shock.

U.S. forces will probably retain overall superiority and, if necessary, could probably operate and win, even against a well-dug-in force, by using better information systems, superior range and firepower, and operational innovations that would permit the greatest advantage to be wrung from the other side's mistakes. But, in anything other than a must-win scenario, a classic victory may be irrelevant. Until the United States faces a hostile country that credibly threatens it and its closest allies—not likely soon—it is limited by the casualties

it will accept, casualties it is willing to inflict on civilians, and potential third-party casualties inadvertently put at risk (perhaps by enemy WMD). Foes may feel fewer inhibitions (except as prudence dictates). A war that trades life for life (even at unfavorable ratios) would probably be regarded as a defeat for U.S. strategy; one that trades equipment dollar for dollar (even at favorable ratios) is more likely to be regarded by the public as a victory.

Conclusions

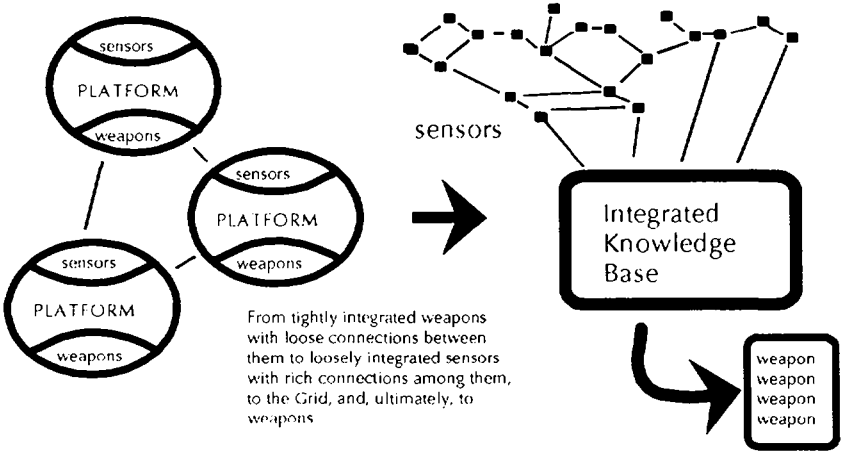
Knowledge has always been useful in preparing operations. Knowing how and where enemy forces are arrayed for attack suggests whether and how to engage them for the best outcome. But once conflict began, other factors—morale, equipment, command, luck—became more important.

The Grid can change the role of intelligence from preparing the battlefield to fighting on it. There is a big difference between spotting armor concentrations and knowing the precise latitude and longitude of each tank, information that can be relayed to PGMs near and far. Intelligence would be able to go directly to operators and, more directly, also to their weapons. The usefulness of detailed illumination would accelerate the shift from local to global information loops. In the Gulf War, the U.S. Army used local loops to find tanks—tank drivers received basic intelligence on enemy dispositions, which helped them find and destroy targets on their own, supplementing their own eyes with tank sensors. In a global loop, enemies are found by combining data from many varied sensors (from space to air and ground, including sensors of the armored group) whose information flows are fused to determine probable targets. Since the Gulf War, shooting at only what an operator sees has started to give way to shooting to coordinates provided to the operator (which, if nothing else, allows the shooter to hide or operate beyond the range at which the target can hit back). This change shifts who gets what information and why.

In this way, the Grid can claim title to the new fulcrum of tomorrow's militaries, as they make the transition (figure 1). Information used to be thought of as support—one more need supplied to warfighters, along with food, fuel, medical services, and

so on. If finding a target is most of what is needed to kill it, information becomes central and strike becomes something provided to warfighters (especially if the target can be hit in many ways by many shooters). Proliferation of basic technology suggests the growing hazards of waging war by moving large forces into battle. Technology makes hide-and-seek warfare both more possible and necessary. The tasks of coordinating sensors, fusing their information, distributing it widely, and supporting joint strike operations illustrate the value of the Grid and suggest its essential characteristics. Although institutions, even the U.S. military, adapt innovations to their own purposes,[47] designing the Grid for new possibilities rather than old doctrine ultimately offers the best path to superiority.

FIGURE 1. ***From platform- to Grid-centric***



Notes

1. Secretary of Defense William Cohen, *Quadrennial Defense Review* (Washington: Department of Defense, May 1997), ii, iv.

2. Oil markets thought so, too. The next day, the price of crude oil on the New York Mercantile Exchange dropped from $32.00 a barrel to $21.44 (10 cents *lower* than before Kuwait was invaded). The price fell only slightly more, to $18.86, by the time Iraq surrendered.

3. The current definition comes from Admiral Owens, former Vice-Chairman of the Joint Chiefs of Staff. See William Owens, "The Emerging System of Systems," *Naval Institute Proceedings* 121, 5 (May 1995), 35-39. In his conception, C^3 networks, sensors, and weapons were equal partners. A Grid that results from C^4ISR integration alone relegates weapons to the outside, consistent with their listening to the Grid but not contributing very much. As weapons develop to have more to tell the Grid, the distinction may vanish. The phrase was used earlier by, among others, General Gordon Sullivan, in *U.S. Army Tech Base Master Plan* (Washington: Department of Defense,1990), and Vice-Admiral Jerry Tuttle.

4. If processor times are indicative (600-megahertz Pentium III of 1999 runs just over 1,000 times faster than the IBM PC of 1981), then performance doubles every 22 months or so. Comparable increases characterize standard desktop PC memories (from 64 kilobytes to 64 megabytes), modem speeds (from 300 to 56,000 bits per second), and hard drives (from 10 megabytes in 1984 to 6 gigabytes in 1999). Some increases are faster: in late 1993, a dollar purchased one megabyte of hard-disk memory; by 1999, it bought 100.

5. The term, invented by Dr. Lee Hammerstrom (Naval Research Laboratory), achieved currency with the 1992 JASON Global Grid Study. The term "Grid" tends, unfortunately, to connote networking (C^4) more than information (ISR) ("building the Grid" suggests connecting everyone rather than building an engine to provide a common operational picture). In DOD, the C^4 and ISR communities speak a different language. To make the Grid work, they will need to learn a common language.

6. A database might include not only a data table but also a knowledge base (a database with rules), text, maps, a real-time video file, or a human analyst accessible through the Grid.

7. Chapter 1 is largely an update of "Technology and Warfare," which appeared in *2015: Power and Progress* (Washington: National Defense University [NDU] Press, 1996). Chapter 2 draws on "DBK and Its Consequences," in *Dominant Battlespace Knowledge*, eds. Stuart Johnson and Martin C. Libicki (Washington: National Defense University Press, 1995), and on "Emerging Military Instruments," in *Strategic Assessment 1996* (Washington: Institute for National Strategic Studies, Government Printing

Office, 1996).

8. From Philip Morrison and Paul F. Walker, "A New Strategy for Military Spending," *Scientific American* 239, 4 (October 1978): 48-61. For another early treatment, see "The New Defense Posture: Missiles, Missiles, Missiles," *Business Week,* August 11, 1980, 76-81.

9. The RMA has been variously defined as a great change in the effectiveness of warfighting that (1) makes the outcome of wars almost independent of the quantity of military systems in opposing hands; (2) trumps the previous RMA; (3) begins military competition anew, irrespective of advantages gained in the prior era; (4) changes basic understandings of the battlespace; or (5) alters relationships among states (suggested by Daniel Gouré of the Center for Strategic and International Studies).

10. PGMs include tactical missiles, torpedoes (and torpedo-based mines), and steerable munitions powered by gravity or momentum (such as laser-guided bombs).

11. Do these technologies favor offense or defense? If offense is the ability to destroy things, then they favor offense. If offense is the ability to occupy another's land, then they favor defense in that the instruments of forcible occupation are visible while moving.

12. A sufficiently stable air platform whose location, bearing, and atmospheric environment is known can often deliver an unguided bomb to within a few meters of a point.

13. Within a few years, fiber-optic gyroscopes used in inertial navigational systems may cost less than $15,000—a third the cost of the predecessor technology, the ring-laser gyro. Current versions are accurate to only 1 degree per hour of flight; they can put a PGM travelling at Mach 2 (640 meters per second) within 6 meters of its programmed destination after flying 40 kilometers. A drift rate of 0.01 degrees per hour may be technologically feasible and would allow a Mach 1 PGM (320 meters per second) the same accuracy after a ride of 280 kilometers. See Philip Klass, "Fiber-Optic Gyros Now Challenging Laser Gyros," *Aviation Week and Space Technology,* July 1, 1996, 62-64.

14. Another $15,000, as the cost of the Navy's Skipper missile demonstrates, can buy sufficient rocket propulsion for a 10- to 20-km standoff boost.

15. Robert Holzer, "U.S. Eyes Rapid-Strike Tomahawk," *Defense News,* April 21, 1997, 1. The Block IV upgrade of the Tomahawk cruise missile is being engineered for in-flight (but not necessarily real-time) retargeting.

16. Even so, designers are looking at UAVs that can withstand acceleration of 15 to 20 g's and so can outmaneuver many PGMs. See David Fulghum, "Pilots to Leave Cockpit in Future Air Force," *Aviation Week and*

Space Technology, February 5, 1996, 26-28.

17. Architects envision a theater missile defense with three layers. Airborne lasers would intercept missiles in boost phase (a $1.5 billion contract was awarded to Boeing for a prototype). High-altitude missiles would be intercepted by upper-tier missiles: the Navy's Area-Wide Standard Missile, the Army's Theater High Altitude Area Defense missile, which failed its first six tests before succeeding and scored 0-for-4 in tests through early 1998, and the well-tested but immobile U.S.-Israeli Arrow. Low-altitude intercepts would be conducted by other missiles: the Patriot PAC-3, the Navy's Lower Tier Standard Missile, the U.S.-European Medium Extended Air Defense System, or the Marine Corps's Improved Hawk. The advantage of complexity is robustness against a threat that can elude one defense. Successive handoffs of the battlespace picture and engagement responsibilities among Air Force, Navy, and Army systems will test joint interoperability. Missile-defense issues are the subject of *IEEE Spectrum* (September 1997) and *Aviation Week and Space Technology* (February 24 and March 3, 1997).

18. Scuds are relatively easy targets because the warhead stays with the body. A Chinese DF-15 warhead, which separates from the body, presents a smaller radar signature, putting it beyond the capabilities of the Patriot. Hua Di, quoted in Michael Dorheim, "DF-15 Sophisticated, Hard to Intercept," *Aviation Week and Space Technology*, March 18, 1996, 22.

19. David Fulghum, "Cruise Missiles Becoming Top Proliferation Threat," *Aviation Week and Space Technology*, February 1, 1993, 26-27.

20. Roughly half the location error derives from local atmospheric and ionospheric distortions between the satellite and user. DGPS can correct for this difference, but the value of the correction decreases as the distance between the user and the DGPS transmitter increases.

21. The cost of antijam capabilities for the JDAM has been estimated at $10,000 per unit. Pat Cooper and Theresa Hitchens, "GPS Jamming Dulls U.S. Smart Bombs," *Defense News*, June 19, 1995, 1.

22. This method will not defeat a jammer that sits between the receiver and satellite, but the GPS constellation is highly redundant (four to six satellites are always available from any point on the ground).

23. Some sensors, for instance, can be used in the same way in war or peace, while others intrude into another country's airspace or territory and must be used with care lest their discovery put their owners in trouble.

24. A sea of devices—sensing, emitting, communicating, redirecting, cuing, filtering, pinpointing, classifying, and determining targets—each segregated as an Air Force, Navy, USMC, or Army asset, each reporting up the separate chain of command, is not the best architecture for data fusion,

hence battlefield illumination. Sensors in the air and space are increasingly joint, but platform, weapon, or distributed sensors are still tied to individual services.

25. Meter-resolution surveillance could be used to cue and track. More precise reconnaissance satellites could be used for identification.

26. See David Fulghum and Joseph Anselmo, "DARPA Pitches Small Satellites for Tactical Reconnaissance," *Aviation Week and Space Technology,* June 9, 1997, 39.

27. A handheld imager carried by a shuttle astronaut flying at 350 kilometers above the earth (higher than surveillance satellites usually travel) has photographed the earth at a 10-meter resolution in relatively low light. Cheri Privor, "Army Imager Flashes in Test from Space," *Defense News,* July 24, 1995, 6.

28. The Sender, a UAV built by the Naval Research Laboratory, has flown a 1-kilogram payload for 2 hours at 80 kilometers/hour. Potential bidders have priced it at $4,000 (payload excluded, unit quantity in the thousands). If forthcoming engineering work on lithium-peroxide batteries is successful, 10-hour flights may become possible. Smaller UAVs are in the works. One UAV (yet to fly far) is the size of a paperback book and can carry a 15-gram load—enough for a miniature camcorder-quality, black-and-white television camera. See Warren E. Leary, "Tiny Spies to Take off for War and Rescue," *New York Times,* November 18, 1997, C1.

29. The Army's Remotely Monitored Battlefield Sensor System can detect a nearby object's passage by using acoustic/seismic, IR, and magnetic means. Human analysis permits estimates of, for instance, a column's speed and vehicle count. Such devices may be more useful if they cost far less (so that they would not be restricted to obvious lines of entry), were better integrated with other sensors (such as UAVs), could be distributed from afar (today's versions require people to place them), communicated more (a precisely timed acoustic signal could support location and identification analysis), and fed generic systems, rather than specialized receivers incapable of further processing. URL:www.atsc-army.org/cgi-bin/atdl.dll/fm/34-10-1.

30. One idea for clearing mines is to use a constellation of "robocrabs" (roughly the size and cost of a desktop computer) to clear pathways in shallow waters. See Pat Cooper, "Robotic Crab Offers DoD New Advantage over Surf Mines," *Defense News,* April 24, 1995, 12.

31. The greater the coverage by any one sensor, the more information it has to transmit. With more information, more energy must be generated, risking an increased IR and radio-frequency signature and, thus, a greater chance of detection.

32. No matter how stealthy a ship may be, a SAR image that shows a blank spot where wave patterns are expected suggests something was seen. To some degree, this applies to stealthy armor and helicopters. The Russians claim their radars can detect stealth aircraft by looking for "holes" in reflected radar noise (see James Asker, "Washington Outlook," *Aviation Week and Space Technology,* December 9, 1996, 23.

33. The U.S. Army brought equipment to Bosnia that could, by tracking the heat of bullets, supposedly detect the source of sniper fire. Earlier equipment could detect quickly and accurately the source of ballistic rounds, such as mortars or artillery shells. William Scott, "Sniper Detector Revived for Airborne Use," *Aviation Week and Space Technology,* August 26, 1996, 64-65.

34. Does stealth have a future? Some officials argue that new composites and coatings can make aircraft almost invisible to radar, eyes, and IR detectors. David Fulghum, "Cruise Missiles Becoming Top Proliferation Threat," *Aviation Week and Space Technology,* February 1, 1993, 26-27. Others contend that the proliferation of Russian-built SA-10 surface-to-air missiles (SAMs) spells the end of stealth. James Asker, "Washington Outlook," *Aviation Week and Space Technology,* August 12, 1996, 23.

35. The Air Force thinks it can speed up finding Scuds by adding IR capabilities to reconnaissance aircraft (see Frank Oliveri, "AF Analysis Targets Missile Launchers," *Defense News,* January 8, 1996, 6.

36. Even if Saddam Hussein had been aware of the uses and effect of information technology, he may also have been aware he could not exploit it without giving lower echelons and experimenters a freedom incompatible with his brand of top-down command.

37. As electronic commerce moves onto the Web, any country (even one under blockade) can get its software cast into a chip in any silicon foundry.

38. Since the mid-1980s, a U.S. company has exported digital-imaging systems that can collect high-resolution imagery 50 miles to each side with real-time data links to ground locations.

39. A 35-mm digital camera that can produce a 3000 x 2000 image costs less than $30,000. See Otis Port, "Digital Finds Its Photo Op," *Business Week,* April 15, 1996, 71-72. Cameras that produces an 1800 x 1200 image had a street price of $700 in late 1999.

40. Larry Armstrong, "Not Just a Blip on the Screen," *Business Week,* February 19, 1996, 64-65.

41. Remotely detonated mines caused a few U.S. casualties in Somalia. A remotely controlled videoscoped rifle, for instance, may make tomorrow's urban battlegrounds even more dangerous.

42. Imagery satellites have been licensed by the U.S. government with the proviso that the cameras not take pictures of certain areas even if so asked (Congress excluded all of Israel, for instance).

43. France has been working with Germany (at least on paper, if not yet in real budget dollars) to launch the radar-based Horus and the Helios 2 (with electro-optical imaging to 1 meter).

44. Vipin Gupta, "New Satellite Images for Sale," *International Security* 20, 1 (1995): 94-125.

45. Matching an item's signature to its template is important to identifying targets, interpreting electronic intelligence, and defeating cover, concealment, and deception. David Fulghum, "DARPA Looks Anew at Hidden Targets," *Aviation Week and Space Technology,* January 6, 1997, 56. Visual (what a target looks like) and electronic templates (what signals it sends out) are well understood and can be built from readings acquired by long-range sensors in peacetime. Heat, noise, and chemical emissions may be hard to sense from far away, and corresponding sensors may not be able to approach adversary equipment in peacetime. Thus, equipment templates may lack short-range components. In war, such restrictions do not hold. Short-range sensors can be scattered near the suspected locations of an adversary's equipment. As they acquire readings correlated by more traditional sensors or direct human observation, the templates can be refined. This refinement increases the value of the short-range sensors.

46. In "From Wires to Waves," *Forbes ASAP,* June 5, 1995) George Gilder describes the Steinbrecher MiniCell, a cellular base station that can fit into a briefcase.

47. And never so quickly as technologists advocate. Because many ill-conceived and unproved notions jostle for attention, a certain conservatism is to be expected, especially with mistakes often fatal to warfighters and, sometimes, to civilizations. See Eliot Cohen, "A Revolution in Warfare," *Foreign Affairs* 75, 2 (March–April 1996): 37-54.

2.
Implications

The advent of the Grid and its role in supporting new methods of warfighting have implications for the use and organization of military power. Three are worth noting:

- The development of standoff warfare, which focuses not on controlling territory but on destroying adversaries (particularly their heavy equipment) through a cycle of scan, sort, sift, and strike, conducted from long range or very quickly and with little trace
- The exploration of two new types of coalitions, one built on a common Grid melded from each country's C^4ISR assets, and another that uses illumination from the Grid to multiply the defense capabilities of a besieged friend
- The attractiveness of mud warfare (low-intensity conflict in a dense environment) to potential adversaries as a response to the difficulty of undertaking conventional aggression in an illuminated world.

These possibilities ought to shape the Grid: if organized knowledge is the military's new fulcrum, the Grid must be ubiquitous, integrated, and widely accessible. Standoff warfare requires detailed, real-time information about the battlespace along with robust connectivity. U.S. support for new coalitions requires the Grid to be scalable, interoperable, and adaptable to non-U.S. users. Mud warfare calls for a Grid capable of discriminating the "what" in the "what's where?"

Standoff Warfare

The ability to see the battlespace clearly and quickly and pass the right information to the right warfighter at the right time can change how the United States goes to war. The last chapter discussed how precision weapons could change conventional warfare from force on force to hide-and-seek. If sensors let warfighters "see" well enough and far more safely from a distance, then why go close? The extent to which operations from standoff distance can substitute for close-in warfare[1] depends on whether long-range strike can be substituted for direct fire weapons.

Some Cost Considerations

Even over an illuminated battlefield, the superior efficacy of standoff strike depends on how fast and cheaply things can be struck from a distance. If weapons are costly, few are made and those few are reserved for the most critical targets. Weapons with long flight times fare poorly against fleeting targets (aircraft, anything taken down or moved after being fired, vehicles that hop from cover to cover).

Most methods of standoff strike are expensive. An F-117A stealth attack aircraft costs $50 million and can deliver, at best, only four bombs a day in two nighttime flights (the aircraft are visible in daylight). The B-2 has 10 times the loadout but at 10 times the cost. The F-22 will cost $100 million. The Joint Advanced Strike Technology aircraft is touted as cheaper than the F-117A but has yet to be built in quantity. Between runs, considerable work is needed to maintain the stealthiness of the aircraft. Advocates of stealth argue that aircraft need not be invisible, merely that they be unseen until close to their targets. But weapons equipped with faster sensors and fire-control computers may hit such aircraft even if given less time to do so.

Cruise missiles can be launched with less preparation time than aircraft need; the newest model (the Tomahawk Block IV) has a unit cost of $575,000, but its warheads are limited and cruise missiles are vulnerable to look-down, shoot-down systems. The ships that fire them are not stealthy, and submarines, which are stealthy, are expensive and cannot carry many.

Medium-range ballistic missiles can be shot from land or, soon, sea. A multiple launch rocket system can put an unguided munition 32 (and soon 45) kilometers downrange for $10,000 a shot. The Army Tactical Missile System (ATACMS) boasts ranges beyond 100 kilometers. Very-long-range ballistic missiles can be fired from anywhere on earth but will be expensive ($10,000 per kilometer at least), unless and until reusable launch vehicles prove feasible and economical.[2]

Electromagnetic guns have been mooted as ways to strike targets repeatedly at long ranges without incurring outrageous costs. But guns need projectiles with electronics that can withstand the shock of being fired and barrels that can be fired many times between overhauls.

Space-based lasers used against ground targets offer the advantage of nearly instantaneous response, but their deployment may infringe on treaties and their beam strength attenuates rapidly in the atmosphere.[3] Targets can be protected with smoke and other obscurants as well as with mirrors. Large guns and powerful lasers tend to be immobile and difficult to hide and are therefore themselves vulnerable. Whether either will be ready within 20 years is another issue.

Striking from medium standoff ranges (20 to 60 kilometers) offers more alternatives and quicker sensor-to-shooter-to-kill cycles. The Raptor missile, an AGM-130 lofted from aircraft, and the Joint Standoff Weapon all boast 60- to 80-kilometer ranges.[4] In the future, it may be possible to mount a missile on a UAV and fly both to medium standoff range. Because UAVs are small to begin with, they can get past air defenses without being so stealthy. If UAVs survive the return trip, fine, but if they are cheap enough, they can be easily replaced. Loitering missiles or weaponized UAVs must both get past difficult engineering problems. Tacit Rainbow, a loitering antiradar missile, was canceled in 1991 after several years of development (and persistent software difficulties). Remotely controlled ground-based missiles offer the advantages of rapid delivery from short distances, thus the destruction of fleeting targets, and little risk to shooters, but their use requires either initial control of the terrain or a surreptitious method of delivery and emplacement.

By now, there are very few targets that U.S. forces would attack with dumb rounds if their location were known precisely. Targets that can be inferred but not pinpointed—infantry units,[5] hostile fire, or scattered soft logistics sites—may still need to be attacked with dumb rounds (bombs, artillery rounds, small-arms fire). Using dumb ordnance at a reasonable cost, though, requires survivable in-theater delivery systems. B-52s will remain useful only if U.S. forces can target enemy radars and adversaries cannot come up with other ways to track such bombers with other ways such as bistatic radars or networked microphones. Keeping U.S. artillery hidden will mean a close contest between U.S. operational stealth and an opponent's UAVs and other sensors.

Even in a world of continually cheaper electronics, long-range strike will probably remain expensive and of limited use against evanescent targets because of the limits of mechanical systems and chemical fuels. The United States is rich and can throw expensive munitions after cheaper targets—but only up to a point. Long-range precision strike is cost effective against military platforms; shorter range weapons (below 60 kilometers, and preferably below 20 kilometers) are for attacking transport vehicles and infantry.

Standoff warfare should be seen as a way to limit the exposure of shooters to conventional weapons and reduce their vulnerability to WMD, but it does not obviate the need to operate near the theater of conflict, if not necessarily in it.

What Standoff Warfare Can Do

In the Gulf War and again in Bosnia, U.S. forces demonstrated that standoff weapons can eliminate key fixed facilities. U.S. forces are developing the ability to use such weapons also to strike moving targets. Standoff warfare may make it harder to push obviously military platforms across clearly forbidden and well-monitored terrain (if enough PGMs were at or sufficiently near the front to destroy them). An obvious invasion would rapidly light up the defenders' screens with targeting information that could be fed to a variety of potential shooters. Were attrition high, the invader might be turned back. Even if invading forces were to push on, defenders (those from the country under attack) would be aided by extremely detailed

information about the battlespace and could therefore wage close-in combat against surviving enemy forces, thinned and stripped of heavy assets (heavier equipment is usually more visible in clutter and more easily distinguished from civilian equipment). Were allied forces inadequate, the stakes high enough, or treaty commitments to apply, U.S. forces, such as ground units, brown-water naval contingents, or close air support, might be called on. In other cases, local defenders may profit from U.S. information flows and the inevitable assistance of special forces.[6]

Key to this strategy is the need to engage enemy units as quickly as possible, before they can secure initial objectives, blend into the background, or dig in against counterattack. For this reason, the Grid (and supporting weaponry) needs to be extended to threatened zones quickly with the goal of striking within the first few hours of an aggressor's violating a border. The threat of effective rapid response could frustrate and thus deter a conventional snatch-and-grab invasion, such as Iraq's 1990 invasion of Kuwait or North Korea's 1950 move south).

In some cases, the United States may not intervene at the outset of the invasion[7]; in others, the initial standoff strikes may not be enough to turn the invasion back. Standoff warfare must then work against dug-in enemies. Once lines harden, enemy progress may be slow; bursting forth with armor and other platforms is risky, particularly if they can be attacked by volleys of hidden missiles wired into the Grid. In face of an initial attack, the Grid needs to support many simultaneous counterstrikes. Once lines harden, the number of strikes declines (so coordinating them is less work), but the Grid would then need to sift through data even more finely to differentiate dug-in enemy assets from civilian or neutral assets and would need to inform shooters speedily of anything that must be engaged.

The empty, quiet battlespace—the slow chess game between competing information systems—may be more typical of future conventional combat than mass melées, particularly if communications permit adversaries to concentrate firepower without massing forces. For both sides, survival depends on knowing exactly what the other side sees and what is unseen and thus might get through. Barring direct observation (having spies inside computer or

command networks), enemy waters might be baited with various worms in order to learn which are bitten. An enemy may know in advance, for instance, that a PGM homes in on a tank's noise and heat emissions. Can that enemy devise a warm, noisy, decoy or will it find that the PGMs it must evade use other signatures, which then must be in the decoy? Will such a weapon be fired against individual tanks, or does it wait for a tank column? Would some tanks be allowed to advance unimpeded, in hope that the enemy might believe it has fooled the Grid? Both sides would want to suppress equipment signatures so that nothing could be identified or located. Most successful engagements would then arise from occasional but fatal mistakes that revealed live targets.[8]

Both the Defense Science Board[9] and the Marine Corps (through its Sea Dragon concept) have explored the battlefield potential of small, highly mobile, lethal units. Marines, for instance, would "infest" enemy territory (rather than storm ashore), assess enemy terrain, find and rank targets, and call for fire from offshore. Yet in an increasingly wired world, especially outside large cities, the movement of any American, particularly one dressed for combat, is likely to be noticed—and thus reported. Further, although forces can be inserted at a choice of time and place, they must be extracted (at a specified place) before supplies (typically, 2 weeks' worth) run out.

How will U.S. forces end conflicts? That depends on how urgent victory is. A siege strategy might be sustainable if U.S. forces had the time to thin opposing forces through precision attrition. Adversaries that could neither break out nor be supplied might do mischief but would slowly have to give in. Partitioning a battlespace into smaller and smaller cells might permit local or ground forces to control successive areas by sweeping through with overwhelming force. Yet controlling each cell would require dense surveillance of interstices. If the threat of adversarial forces crossing from one cell to another were noticed within minutes, those forces could be confronted by forces in large numbers. Legitimate traffic must be identified so it may pass. A ground presence without precise ground knowledge and the ability to respond and move quickly will leave thin forces exposed, a recipe for casualties (or excessive collateral damage).

In other circumstances, U.S. forces may need to counterattack to end a war quickly, despite the difficulty of doing so against an enemy dug in and itself equipped with robust fields of sensors and PGMs. Ground forces can smoke out well-dug-in or hidden adversaries, much as hunting dogs flush quail. When the adversary is surprised or incompetent, this move works well, but it can also produce many casualties (as in search-and-destroy operations in Vietnam). U.S. forces might also define a series of limited objectives that can reinforce one another, seize them quickly, and burrow into the terrain or hide against the background of a friendly or at least, neutral population. The techniques of information warfare, in particular good assessment of the speed of an adversary's reaction cycles and the quality of its communications, will play a large role in offensive operations.[10] U.S. forces will prosecute moving and fixed targets differently: moving targets are visible because they move; what is fixed may be searched for in detail. Scouring for weaponry (short-range missiles and mines buried in clutter, for example) will remain difficult. Within 20 or 30 years, U.S. forces may be able to use small, somewhat mobile sensors to detect suspicious objects for inspection.

Standoff Warfare as Deterrence

A capability for standoff warfare poses a dilemma for potential bullies. Units and assets heavy enough to coerce and conquer neighbors may be easy targets for U.S. forces, because they are more easily identified. Light forces can use infiltration and subversion to slip by unnoticed and thereby preempt or, failing that, at least tax a U.S. intervention with a constant rain of casualties. But units and assets so light may be not be able to outgun the bully's neighbors.[11] As the difficulty of choosing between the two structures increases, so, too, will regional stability. The need to fund two forces aside, the command, control, and culture of a heavy military that works through shock may mesh poorly with that of a light military that works through stealth.

Van Creveld argues[12] that conventional warfare among established countries has not mattered much during the past 50 years and will matter less in the future. Bullies unable to use invading forces will find other ways to intimidate neighbors. Even if true, the ability to thwart direct aggression remains worthwhile. The argument that

standoff warfare will not stop enemies that can move in the mud when roads are denied them ignores the extent to which mud raises the cost, time, and friction of operations. Denying adversaries certain avenues can mean channeling them into others where traditional killing power can be concentrated.

The imminence of destruction can be more convincing than its eventuality. An Iraqi tank force, having just picked off Kuwait, may strike enough fear into Saudi Arabia to influence its oil marketing to Iraq's liking. Were Iraq to rely on slower means (such as low-intensity combat) to make its point, coercion would lose much of its psychological power. Because war may be used to make coercion believable, anything that reduces the credibility of coercion could limit the motive for conflict.

Standoff warfare may offer greater deterrence in tomorrow's putative Asian conflicts than in European scenarios. Many Asian countries either are islands or sit at the end of peninsulas. Seaborne invasions are far harder to hide than ground invasions. A naval blockade, one alternative to invasion, cannot bring quick victory, and its impact on civilians may generate a flow of refugees and bad press. Success requires a large, expensive blue-water submarine force (or very-long-range rocket and missile bombardment). Asian countries may be ripe for rivalry among themselves,[13] but because they lack the means to convert rivalry into successful warfare (such as taking and holding land), the United States may never need to assume the same broad goal-line defense role against a potential Asian hegemon as it did in Europe during the Cold War.

Versus WMD

While the United States is building its Grid, adversaries (like Iraq, Iran, Syria, and North Korea) are busy catching up with an earlier RMA, nuclear weapons and its poor cousins, biological and chemical weapons. The Grid cannot trump WMD (nor is it a good argument for unilateral nuclear disarmament), but by removing tempting targets from the battlefield and permitting force to be used more discriminately, the Grid can reduce the impetus or the temptation to use WMD.

Were a foe to abjure conventional means entirely and wish to pursue WMD terrorism, the Grid, although no guarantor of protection, might offer help. Good eyesight would help the United States to identify and take out sites of WMD production and deployment and make it easier to shoot down ballistic or cruise missiles that deliver WMD. Smuggling nuclear bombs on trucks is no sure thing. Those forced to use less reliable delivery methods may calculate that, although the odds of success decline, a failure discovered might still induce devastating retaliation. Ultimately, nuclear deterrence may have to be used.

The Grid may do better at forestalling WMD usage on the battlefield. The effect of enemy use of WMD to back up conventional forces would decrease if standoff warfare permitted putting fewer U.S. forces at risk. Its political effect as blackmail also might be diluted, perhaps below the point where its use is worthwhile.

If an adversary held back WMD to protect its core areas, good illumination might permit U.S. forces to win without entering sensitive areas. Typically, seeing enemy supplies is hit or miss, and hunting for them must take place along the length of the enemy's supply lines and deep into its territory. Were supply lines seen more reliably, the United States could wait until supplies were closer to the battlefield, confident that they could be destroyed.

In general, good illumination may dampen a potential action-reaction cycle that culminates in the use of WMD.[14] If the Grid keeps neighbors focused on facts rather than on fears of what is brewing just beyond their borders, the neighbors could choose to wait for incontrovertible evidence of aggression, rather than jump the gun. Where evidence is ambiguous, nonlethal weapons can be used (to tag weapons, for example, or disable their electronics) against forces the Grid could see in detail (for targeting and damage assessment). Instant response with nonlethal weapons would carry less risk than the use of lethal weapons alone offer. If the assessment is incorrect (for instance, what looked like preparations for an invasion were just normal redeployment), both sides could back down and still save face.

A New Calculus for Force Requirements

Forces tend to be sized and structured on the basis of estimates of the number and size of the enemy. Debates on the plausibility of two nearly simultaneous major theaters wars (MTWs) dominated the Bottom-Up Review in 1993 and the Quadrennial Defense Review (QDR) in 1997. The credibility of an MTW threat may fade (for example, North Korea may implode). If so, the need to justify forces more than enough to meet the residual threat introduces the issue of against whom else might the United States be arming—Russia? China?—and whether such planning becomes a self-fulfilling prophecy, all of which constitute a hazard of threat-based force calculation.

Hide-and-seek warfare suggests another way to assess the adequacy of the U.S. military, one largely unrelated to the size of the enemy's forces (so no specific enemy need be named). Combat, especially standoff combat, consists of three elements: seeing, striking, and moving sensors and weapons to where they are needed (which is what platforms do).

The cost of illuminating a battlefield is only modestly related to its size and even less related to how large the other side's force may be (requirements for space assets, for example, are unrelated to the size or location of the area to be viewed). The cost of establishing a worldwide Grid may be large, but the cost of a working inventory to resupply sensors, emitters, and other nodes in war may be cheap. Only weapons requirements are related to the size of the enemy, but weapons account for only 1 percent of today's defense budget (having peaked at 3 percent in the mid-1980s). Finally, the cost of hauling sensors and weapons near to but not into harm's way is modest compared with the cost of most of today's platform-based forces.

An adversary's sophistication at hiding or disguising its assets, rather than the number of those assets, drives up density of placement, power, and discrimination of sensors used to detect and classify them and thereby drives the cost of C^4ISR. In the face of information warfare, the United States must reinforce its network architecture: take pains with computer and other information security, use encryption and antispoofing techniques all the time, use jam-resistant and overlapping radio communications, harden and multiply

critical nodes and paths, and prepare to recover system capabilities as components are destroyed or disabled in combat.

Another factor driving C⁴ISR costs is the distance between the target of observation and U.S. operational areas (including international waters)—central Asia costs more to monitor than Korea. UAVs capable of a several thousand-mile round trip cost more than those that need go only a few hundred miles. The delivery of sensors from afar (whether by aircraft or artillery) is more problematic, and longer transit times to the theater lengthen the odds of accident or interception. Aerostats cannot see beyond a few hundred kilometers. Radio networks are even more difficult to maintain over long distances.

Distance also raises the cost of strike. A nearby target can be engaged with short-range missiles, lofted glide bombs, or even artillery (such as land- or sea-based ATACMS), but distant targets require medium-range missiles, which in turn require large engines or rockets, or both, and more expensive flight-guidance systems. The longer the flight times, the harder it is to attack evanescent targets and the more opportunities there are to be shot down. Many U.S. aircraft lack the range to attack targets more than 500 kilometers away.

Holding distant targets under constant observation and at risk may require platforms that can get sensors and weapons close to the targets. The ability to control and operate in international waters is very important, as is a sufficient complement of long-range aircraft, whether or not they operate from standoff ranges or close-in ranges. Table 1 summarizes these considerations.

Coalition Structures

A Grid that can be extended to allies of both comparable and lesser capabilities offers new types of coalitions to meet U.S. needs. For instance, countries allied with the United States are concerned that the effect of the Grid will be to make the U.S. military so high-tech that its allies will no longer be able to fight alongside (much as a battle group cannot easily combine slow and fast ships).[15] The validity of this fear depends on how alliances work. In Cold War Europe, nations had their own sectors to guard. In May 1996, the North American Treaty Organization (NATO) recognized the U.S.

preeminence in C⁴ISR and strategic lift and conceded that U.S. intelligence, long-range lift, and strike capabilities may let other countries conduct operations beyond the borders of member states.[16]

TABLE 1. ***How threats affect force requirements***

(**XX** = strong, **X** = modest, blank = nil)

Force Requirement	*Characteristics of Threat*			
	Number or Size*	Acreage**	Sophis-tication	Remoteness
Global C⁴ISR		X	X	
Local C⁴ISR		XX	XX	X
Weapons	XX		X	X
Lift	X	X		XX

* Number of opponents and size of their armed forces

** Size of monitored battlespace

Another way to envision future coalitions is to consider the Grid as a utility[17] to be used by any alliance member with ever less expensive plug-compatible appliances: receivers, workstations, fire-control systems, targeting modules, and software in general. Many allies already own digital hardware, and some have the rudiments of a Grid in place or under construction.

Allied capabilities can be melded to the U.S. Grid in two ways. Each ally with its own Grid might forge system-to-system links with the U.S. Grid, creating, in effect, a larger Grid (just as the union of two Internets is a larger Internet). Alternatively, allies could connect their sensors, databanks, processors, and fire-control units to the U.S. Grid much as U.S. components[18] are connected. Systems designed by allies to work with their own Grids may need updated software to work with the U.S. Grid, to take advantage of the Grid's information and services, and to meet the Grid's expectations for connectivity. In

time, allies may even build hardware and software hooks to connect to the U.S. Grid as easily as to their own.

In a seamless allied Grid, which components (sensors, switches, processors, or knowledge-bases, for example) were owned by whom ought to matter less[19] than such features as reliability, accessibility, interoperability, and security. Data from a British UAV electro-optical sensor can be linked through a U.S. network to readings from Dutch microphones, so that the data flows can be fused with the help of a French-hosted software agent and compared to a German-provided database of marine templates to provide targeting guidance to a topside gun on an Italian Frigate. A NATO Grid could conceivably include civilian elements and commercial elements. Although others may believe their own assets first (assuming they know what information comes from where), the Grid can be designed so that technology will not foreclose using the assets of others.

Bytes versus Bombs

When alliance commitments are not at issue, the U.S. public tends to shy away from military operations that risk many casualties.[20] As far back as the French Indochina War, U.S. strategists pondered air strikes to influence conflicts with little risk to forces. But the Vietnam War showed the U.S. public is very sensitive to the capture of U.S. airmen. Extended use of aircraft requires near-theater presence and large overseas deployments. Air strikes also put the onus of conflict on the United States and raise the risk of terrorist counterstrikes.

Illuminating the battlespace for others could avoid these problems while deterring conflicts or influencing outcomes in accord with U.S. values (ensuring aggression does not pay) or interests (preventing the establishment of a rogue state). Illumination could be offered with few fingerprints (important when overt involvement might cause trouble or lead others to ascribe an implicit commitment of U.S. prestige). The United States already offers data collected from satellites. To this it could also add data collected from UAVs, over-the-horizon radars, standoff naval sensors, and ground sensors, delivered as imagery or populated battlespace maps (showing targets in real time).[21] To bring allies' information systems and operators up to U.S. standards, further support might include simulation packages, systems management

software, and network assistance. The Grid's hardware and software could fuse information from sensors in a host's general population (such as videocameras and cellular phones) and wring information from previously unusable data. Host forces could supply human observation, ground presence, and command, as well as fire weapons.

In theory, the United States could never show up at all; in practice, it would probably provide special operations and liaison support,[22] if not air cover and arms transfers. Table 2 suggests parallels between the transfers of arms and information that increasingly favor information.

Applications

Four hypothetical cases show how information support can be useful: preparing nations for alliance membership, helping friends conduct their own standoff warfare, exercising covert leverage, and keeping friends on their side of a border.

Candidates for NATO membership, for instance, are already receiving help with their C^{4}ISR systems to enhance their capabilities and to facilitate their ultimate integration into NATO systems.[23] Giving them real-time information flows on top of such help would let them see potential trouble more easily. Although alliance membership is binary (one is either in or out), information assistance is continual and can be offered piecemeal to specific countries. To achieve interoperability, the United States might, for instance, reveal more of the Grid (its contents and capabilities) to the Slovenians than to the Russians. If a crisis were to demand that new countries be brought into alliances quickly, early preparations would ease their integration into appropriate military structures.

U.S.-supplied illumination could reduce the pressure for immediate direct U.S. intervention. A Kuwait could defend itself by installing medium-range, point-guided PGMs (perhaps hidden in 10 times as many desert holes). The invader's assault forces would be identified as targets with precise, real-time locations that could be passed on to individual weapons. When Iraq threatened to return to Kuwait in 1994, the United States mounted Exercise *Vigilant Warrior* in response, which cost almost a billion dollars. Such an investment

could buy enough munitions (plus cover the cost of training) to do the same mission for a far longer period.

TABLE 2. ***Transferring arms or information***

Arms	*Information*
Add to ally's arms	Multiply effect of ally's arms
Can be interdicted in war; hazardous to protect	Can be protected by redundancy, encryption, and spread spectrum
Can be misused	Can be shut off if misused[24]
Can be diverted	Can be shut off if diverted
Reduce provider's assets when transferred	Can be copied
Difficult to ship in secret	If encrypted, can be decrypted only by insiders
Value-neutral	Suggests what provider thinks is worth looking at

Illumination can help one side (an example would be the Bosnian Muslims) without impelling powerful countries to intervene on behalf of the other. The effect of friendly artillery would be enhanced if the exact location and track of opposing artillery were revealed. A major power friendly to the other side may suspect its friends are being hurt by the United States but, because the support is covert rather than overt, may feel less political pressure to respond.

Information may help allies to protect themselves against hostile infiltration without crossing into another country (such as Turkey's 1995 pursuit of Kurdish rebels into Iraq). Data collected remotely can substitute for costly and risky border patrols—and, unlike patrols, the cost effectiveness of such surveillance rises every year with improvements to digital systems.

Limitations

Information cannot be helpful until put into a form compatible with partners' systems, weapons, doctrine, sophistication, expectations, and rules of engagement. Fielded sensors that provide the information must be matched to the local environment and the characteristics of the expected enemy. What DOD would give should fit how others fight, not only how U.S. forces might.

Consider the ability to identify and lock onto a truck equipped with a Bushmaster-class machine gun. Ordinarily, real-time tracks are flashed to U.S. forces, which then strike from standoff range. Would these data suffice for allies? If their weapons were precise but lacked range, allies would need to fire from close up; they would need to know where other enemy assets lay in order to operate from protected spots. If the allies' weapons also were imprecise, then allies would need reliable, real-time battle damage assessment for subsequent reengagement (preferably before fire was returned). If allies used ground forces to smoke out adversaries, they would need the Grid to find the best way in and out quickly in order to shoot at the vehicle without being trapped in the chaos of small-arms exchange. By contrast, some forces shoot once provided with what they consider sufficient evidence that the vehicle is hostile, rather than wait for certainty beyond the reasonable shadow of a doubt that U.S. forces may require.

Sometimes information is not enough. Friends too small or too weak (the Caribbean or Persian Gulf states come to mind) to maintain serious forces will probably be too small or weak to face serious foes, even when the United States bolsters their forces with detailed illumination of the potential battlespace.

Policymakers may assume falsely that they can intervene in distant conflicts without risk to U.S. citizens because their soldiers are safe. But U.S. citizens are everywhere; once the pot is stirred they may need to be evacuated, an operation that may require forces to descend into the chaos. Inevitably, some people stay and later demand extraction when the hazards of it are even greater. Even if information excites less anti-Americanism than bombs do, adversaries may still retaliate with terrorism.

Relying on information rather than on more committed efforts can reduce the influence of the United States on the ends and means of conflict. Threatened countries may seek friends who will make a greater commitment. Other countries may take what help they can get, but if a country is forced to choose between standing up to a bully or deflecting its wrath toward a neighbor, a U.S. commitment to that country might make a great difference to collective regional security.

Illumination offers great power and little risk, so there is the possibility the United States may intervene too readily. A power unchained by even a small threat of the consequences may make close friends nervous. Secret assistance provided through intelligence agencies can escalate into a deeper entanglement, and the United States could find itself involved in a conflict it might have avoided had it taken the time to reflect. Promiscuous access to precision information can fuel arms races for compatible weaponry.[25]

Others also may offer information, particularly if they do not want to leave evidence of a confrontation, even an indirect one, with the United States. A sophisticated and powerful country that can emulate U.S. C^4ISR capabilities can help its friends practice hide-and-seek or information warfare and so learn what may work against the United States. The possibility of such help is one more reason not to underestimate the sophistication of Third World militaries.

Mud Warfare

Standoff warfare can, at times, assume a Nintendo-like quality: a rapid succession of scan (surveying the battlespace), sift (comparing fused sensor input to signature templates), sort (prioritizing targets), and strike.

Unfortunately, the great U.S. desire to make war only in this way and no other could push foes to find other ways to defeat it, particularly with methods and equipment previously unseen. Foes could try to change the rules of the game by showing up where not expected, mixing in with innocents and friendlies, taking hostages, dragging in third parties, and so on. Foes can seek to work as closely as possible to the shadows (subject, of course, to their own operational requirements), where terrain is densest and illumination

weakest. The U.S. counterstrategy might be to drag the fight toward the greatest imposed (rather than ambient) complexity by proliferating sensors, networked electronics (e.g., cellular phones and videocameras), detectors, monitors, databases, switches, and other nodes. Thus the agility of U.S. forces and their superior systems integration skills may decide the outcome.

An aggressor may seek to achieve rapid conventional effects by methods of low-intensity warfare, acts that may pass unnoticed: infiltrating troops into commercial traffic, organizing crime and terrorism to look like ordinary urban chaos, gathering military intelligence by methods associated with commercial intelligence, exploiting the target's own information-collection systems, and placing real bombs in a country's physical infrastructure and logic bombs in its information infrastructure. At some propitious point, distributed communications (from cellular telephones to tom-toms) may be used to concentrate forces against government targets through devices (pickup trucks and construction equipment), devices that, until used, look and are civilian. U.S. forces alert to such possibilities will need to look for information from the Grid.

Could the ability to illuminate the battlespace alter the outcome of something like the Vietnam War—and, by extension, of tomorrow's low-intensity conflicts and peace operations? A fine-toothed ability to survey even a low-density battlespace and to act quickly against anomalies can inhibit the formation of massed units, cut supply movements, and take rapid advantage of the inevitable mistakes that reveal obvious targets.

Mud warfare is necessarily close-in combat whenever the intelligence required to differentiate signal from background is hard to read without direct contact. Key nodes in Third World cities may not be obvious from standoff inspection. The expertise necessary to distinguish hostile from neutral sites, and the trust required for others to volunteer the right hints, often are impossible to have without also being on scene long enough to learn the territory. Distinguishing civilian assets—such as pickup trucks—from military ones—such as "technicals" like pickup trucks carrying mounted machine guns—is difficult without putting sensors very close to the target or using soldiers to make determinations.[26] In standoff warfare, things are

targets because of what they are (an enemy tank or bunker); close-in warfare is necessary when people or things are targets because of what they do, plan to do, or have. Tracking one technical that did something specific (such as fire on a police station) may be easier than finding a technical among pickup trucks. U.S. soldiers need not risk day-to-day patrols, even if occasionally warranted; locals can do that job. U.S. forces can operate covertly or selectively to drop in at the right place and time to counter emergent force concentrations, such as local militias. This strategy requires an exquisite combination of situational awareness and fast decision times. Situational awareness is important for sensing and understanding the rhythms and cycles of a volatile environment and for adept, small-unit response. Fast decision times are important when potentially opposing forces can cohere into action quickly. Control requires repeated demonstration that coalescing opposition can be engaged and neutralized quickly.

Close-in combat is called for when the goal of U.S. operations is to immobilize or neutralize hostile forces rather than kill them. In Operation *Just Cause* (1989), the United States sought to remove General Noriega from power (and from Panama) but did not necessarily want to punish Panama or destroy its ability to defend itself. Widespread casualties would have complicated subsequent relations with the country. Although military assets such as armored personnel carriers were targeted for destruction, soldiers generally were not. Success in such endeavors often requires physical occupation of military facilities, something standoff strikes cannot do.

Peace operations resemble mud warfare by calling on military forces to operate against a background of day-to-day life. By seeking to suppress the use of force, rather than suppress forces, peace operations differ from war. Usually, visible presence (or its threat) can inhibit violence. Mud warfare happens when the expectation fails. Thus, much of what the Grid illuminates in support of mud warfare must be equally well illuminated for peace operations.

The homelands of United States and its allies are not liable to be threatened by mud warfare. Many key interests, such as freedom of the seas and the security of many oilfields, can be defended without mastering its tactics, and fear of casualties will inhibit the U.S. interest in such combat—yet a Grid built on the assumption that U.S. forces

will never engage in mud warfare is unwise. Even if U.S. forces are not engaged (at least not in large numbers), those of its friends may be, and the U.S. ability to illuminate the battlespace for them may be decisive. A Grid agile enough for mud warfare gives the United States ways to influence the outcome of such conflicts. Given that success often goes to the side that can outlast its opponents, a Grid that permits things rather than lives to be expended month after month has advantages.

Conclusions

The ability to illuminate the battlespace permits the use of standoff warfare as an instrument of power with relatively light U.S. casualties. The further ability of the United States to illuminate the world for others also can be influential, whether or not U.S. forces are engaged. An agile Grid that provides illumination can help either U.S. forces or its friends prosecute mud warfare somewhat more effectively than today. That noted, the Grid must have enough play in its structure to accommodate a future grown bleaker or foes grown more clever than today.

Notes

1. Even the Marines are seeking to increase the typical engagement distance from 1,000 to 10,000 meters. See Robert Holzer, "U.S. Marine Tests May Reshape Corps," *Defense News* 11, 12 (25 March 1996), 37.

2. The ultimate model of rapid response would be a large rocket always on the launch pad, filled with antiarmor projectiles, each with terminal guidance and its own virtual channel to receive updated aimpoints. If a 20-kilogram warhead, reentering the atmosphere at Mach 25, can kill armor, then a single heavy booster (with its 10-ton payload) could disable 500 targets at once.

Whether this is affordable is another issue. The NASA administrator talks of getting to LEO for $2,000/kilogram by using reusable boosters. James Asker, "Washington Outlook," *Aviation Week and Space Technology* 144, 7, February 12, 1996, 19. In support of that goal, in 1996, NASA awarded Lockheed Martin a large contract to produce its wedge-shaped spacecraft (beating out Boeing's shuttle derivative and the McDonnell Douglas DC-X, which launches and lands vertically) for a March 1999 launch. The award will test the claims of some aerospace engineers that reusable launch

vehicles (one of which is the single-stage-to-orbit type) could be available in 10 years for $5 billion. NASA had previously estimated that success would require 25 years and $20 billion. Orbital Science Corporation, whose small boosters are twice as expensive to use per kilogram of payload as large ones, hopes one day to reuse 75 percent of its rocket components, which might drop costs to near $5,000/kilogram. Two start-ups are pursuing a goal of $4,500/kilogram to LEO: Pioneer RocketPlane—William B. Scott, "McPeak, Hecker Head 'Space-Plane' Project," *Aviation Week and Space Technology* March 10, 1997, 22, and Kistler—Joseph Anselmo, "Launchers see Nothing but Blue Sky Ahead," *Aviation Week and Space Technology,* April 7, 1997, 41. A skeptic might recall that the Space Shuttle promised low costs and frequent launches yet, compared with older technologies, yielded few economies.

3. Israel is nevertheless exploring the TRW Nautilus laser for defense against short-range Kytusha missiles after a similar midinfrared advanced chemical laser (Miracl) successfully engaged one at White Sands.

4. DOD is developing two PGMs that reach Mach 6 (2 kilometers/second), one for the F-22, and another to succeed the 1.5 kilometers/second line-of-sight anti-tank missile. With no air resistance, such a missile could fly 400 kilometers.

5. At $575,000 each, a cruise missile seems a preposterous weapon to use against individual soldiers, but the United States fought Vietnam as a war of personnel attrition and, its own casualties aside, spent $1.0 to $1.5 million for every enemy slain. Manufacturing cruise missiles today at the rate at which enemy soldiers were killed then could drop unit costs to $200,000 (an aerospace rule of thumb associates every doubling in quantity with a 20-percent cut in unit costs).

6. The great vulnerability of anything that becomes visible permits defenders to find advantages in retreat (if time and space permit). Armies moving forward must often mass or otherwise reveal themselves while overcoming impediments; their visibility increases if they must advance into well-wired terrain. Armies moving backward encounter less resistance and can move more stealthily. Because they are more visible, attackers take more casualties than defenders. As attack formations are thinned while moving forward, they can become overextended. The Korean War may be read as three advances (North Korean forces in mid-1950, U.N. forces in late 1950, and Chinese forces in early 1951), each followed by total or partial collapse.

7. Why would the United States hesitate? Interest in a particular outcome, or in an end to conflict, may not be sufficient at first. Aggression may also be ambiguous: Are the Viet Cong proxies for a North Vietnamese invasion or armed dissidents? Who held the U.S. embassy hostage, the

Government of Iran or renegade students? Were Bosnian Serbs an aggrieved ethnic group or a front for Serbian control of Yugoslavia?

8. See Stephen Biddle, "Victory Misunderstood: Skill, Technology, and What the Gulf War Tells Us about the Future of Warfare," *International Security* 21, 2 (1996), 139-179. According to Biddle, the lopsided tank battles of the Gulf War have been misread. Had the Iraqis made fewer specific mistakes, both sides might have suffered similar casualties. The character of modern warfare means that the Iraqi mistakes were severely punished. Biddle concluded (1) that training, not technology, made the difference and (2) that those who master constantly rising levels of complexity will be tomorrow's winners. Biddle declared himself skeptical of the RMA, but making the Grid (which would reify the RMA) work would be an exercise in the management of complexity, particularly in helping forces quickly take advantage of an enemy's mistakes.

9. The Defense Science Board *1996 Summer Study Task Force on Tactics and Technology for 21st Century Military Superiority* (October 31, 1996) offers a good treatment of how individual warriors could exploit a dense infrastructure of sensors and processors to raise their situational awareness.

10. When operations depend on networks, operators may be stymied or even defeated when networks fail. The blitzkrieg was invented largely to attack relatively soft targets—mainly the logistics support network—behind the lines. Communications networks are now needed to provide C^4ISR support to modern militaries. Information warfare, by analogy, could attack C^4ISR networks to isolate units from both their data flows and one another. If warriors can understand opposing networks, find weak spots in those networks, and crunch them, they may engineer a collapse. Weak spots that occur each time a network has to adjust to a crisis or opportunity may be created or exacerbated by the other side. Detecting and attacking them before they can be strengthened can lead a network to collapse. This strategy requires the Grid be alert, flexible, and fast.

11. Andrew Krepenevich, who heads the Center for Strategic and Budgetary Alternatives (Washington), has argued that Third World countries have given up trying to replicate the U.S. military with its planes and tanks. Countries like Iran buy cruise missiles, command and control systems, transport, mines, diesel submarines, and in some cases, WMD. See his interview in *Defense News,* October 25, 1993, 30; and George Seffers, "U.S. Army Study: Reduce Force Logistics, Improve Mobility," *Defense News,* December 16, 1996, 8. Such countries seek not to defeat the United States but ward off its intervention. But would the United States intervene in the first place—unless Iran, for example, was taking land, presumably with

equipment such as planes and tanks?

12. See Martin van Creveld, *The Transformation of War* (New York: Free Press, 1991).

13. See Aaron Friedberg, "Ripe For Rivalry, Prospects for Peace in a Multipolar Asia," *International Security* 18, 3 (Winter 1993-94), 5-33.

14. Similarly, the competition of adversaries, each convinced that hesitation would put it at a permanent disadvantage in mobilizing forces, made the descent into World War I impossible to stop.

15. German General Klaus Naumann, who chaired the NATO military committee, fretted that the U.S. military is becoming high-tech with such "unparalleled velocity [that] one day we will see a disconnect between the United States and European Allies" (quoted in James Asker, "Washington Outlook," *Aviation Week and Space Technology,* October 6, 1997, 23. European countries can afford an RMA but they prefer to spend only 60 percent per capita of what the United States does on defense (and even less on defense hardware). In the U.S. view, they lack the will to buy the requisite hardware and software (although size, not just affluence, is needed to afford space assets or a complete system of systems). European governments, for their part, fear that the U.S. lacks the will to shed blood alongside its allies. A military particularly good at standoff warfare may be expected to insist on contributing to a common effort from beyond or above the battlefield, while the Europeans suffer the casualties. But the United States did supply ground forces in Bosnia.

16. The desire to concentrate on C^4ISR and lift while others do the fighting is not a U.S. monopoly. Similar hopes are offered by officials in Australia (see David Fulghum, "Australia's New Defense Strategy: Surveillance, Comm Links Dominate Upgrade Plan," *Aviation Week and Space Technology,* August 25, 1997, 50. To some extent, this hold for Germany (see Jack Hoschouer, "Germany's New Roles Expose Needs," *Defense News* , February 3, 1997, 4.

17. Some now urge the United States to work systematically with European allies in the emerging infrastructure of data dissemination, fusion, and collaborative planning. Dennis Gormley, "Make Information Dominance NATO's Military Glue," *Defense News,* July 8, 1996, 21. In early 1997, eleven NATO nations launched a feasibility study of how they might share command of and battlespace data from their UAVs. Brooks Tigner, "Allies Aim to Share Reconnaissance," *Defense News,* February 17, 1997, 1.

18. Physical and syntactic connectivity need not mean unrestricted access (for example, just because the U.S. Grid is connected to Dutch artillery fire-control systems does not mean that U.S. commanders can fire Dutch weapons). Multilevel security software is designed for such tasks as

compartmentalizing a NATO Grid into national and NATO domains.

19. Who determines how and when sensors are deployed, where they point, or what spectrum they collect is not a trivial matter, particularly if sensors can, for instance, destroy mines.

20. The Gulf War sharply reduced U.S. expectations of casualties in even a major conflict, perhaps faster than technology can satisfy these expectations. Eighteen dead were too many in Somalia; three suicides among U.S. servicemen in Haiti sufficed to draw hostile congressional attention. Imagine a presidential call for a war to save, say, the Philippines from falling to radical forces waging a Vietnam-style guerilla campaign. Our technology, the President continues, can reduce casualties to a tenth of what they were in Vietnam—only 5,800 dead. Few Americans would respond favorably to such a "deal." U.S. forces have become quite careful in places like Bosnia, where standard practice now is to venture forth only in heavily guarded four-vehicle convoys. Casualties are reduced at the expense of a higher operational tempo whose long-run sustainability is untested. This attitude may change if the United States were to face a country big enough to place it in jeopardy. Yet such threats do not clearly proclaim their intentions and capabilities, at least not at first. To dissuade countries from peer-level competition, the U.S. may have to impede their march to power (perhaps by influencing the outcome or inhibiting the outbreak of proxy conflicts that they sponsor) years before the U.S. public will for direct intervention (and thus tolerance of casualties) can be mustered.

21. When a DBS receiver a foot wide can pick up a gigabit per second, raw bandwidth into theater is unlikely to be a major constraint.

22. In 1993, a decorated armor general unexpectedly opined to the author that *Desert Storm* circa 2015 would require a force of 101,000: 100,000 from the Space Command, and 1,000 from the Special Operations Command.

23. Eastern European countries reportedly are using peacekeeping and search-and-rescue operations to determine what to do for compatibility (Brooks Tigner, "East Nations see Peacekeeping as Key Entree into NATO," *Defense News,* January 30, 1995, 20. Jan Sitek, the Slovakian Minister of Defense (interviewed in *Defense News,* June 26, 1995, 54) noted that the nation seeks an information system fully compatible with NATO. Janis Trpans, his Latvian counterpart (interviewed in *Defense News,* March 13, 1995, 30), admitted that Latvia still has large stores of Bloc equipment to be maintained ("buy East") but now wants to "talk West".

24. For instance, NATO was harder on Serbs than on Bosnian Muslims because Serbs were judged to be aggressors. If NATO were to help Bosnia in order to even the playing field, the Bosnians might then be tempted to

become aggressors. To the extent that information support made the difference, NATO might be able to quell ambition; withdrawing arms or negating training is harder.

25. Jeremy Kaplan, of the Defense Information Systems Agency, claimed that if the U.S. can enable point-guided PGMs for its friends, the friends' incentive to acquire them rises. A country so stocked would still want alternative sources of battlespace information. That need would prod other suppliers to improve their battlespace surveillance capabilities to support point-guided PGMs. Many European companies, for example, would not develop a system if they did not expect foreign sales. The result could be an arms race that would vitiate the initial U.S. advantage in the sensor-to-shooter cycle. One way to ensure that a recipient uses only information supplied by the U.S. DOD is to sell missiles that could respond only to data encrypted by the Grid.

26. General Fogelman, the former Air Force Chief of Staff, maintained that "air occupation" is now a feasible and worthwhile low-casualty substitute for ground occupation. Patrick Cooper,"U.S. Stealth Enhancements are Key to 'Air Occupation,'" *Defense News,* September 16, 1996, 1.

3.
Alternatives

Nearly everyone pays lip service to the goal of C^4ISR integration. Some within DOD even accord it first among DOD program priorities.[1] Yet integration, however necessary, is not enough to build the Grid. The depth of integration, the breadth of things to be integrated, and the shape of the result define the Grid—that is, the challenges faced in its construction, and the services and knowledge it provides.

If the progress and the plans made since the Gulf War are considered, then circa 2015, DOD ought to be well on its way to the Grid. Most sensors, weapons, and networks will be interconnected and largely interoperable. Commanders will have a reasonably good picture of a conventional battlespace (if not yet an unconventional one). Standoff warfare will work better (in the right environments) than in the Gulf War or Bosnia. But the Grid DOD may settle for goes only part way toward what it could and, more important, what it ought to field by then.

Such a Grid may be sufficient if the worst problem the military faces is repeating such operations as *Desert Storm* (Persian Gulf), *Just Cause* (Panama), or *Deliberate Force* (Bosnia) against hapless foes. Whether it can illuminate the battlespace for hide-and-seek warfare or help prosecute mud warfare is less clear. Indeed, the different kinds of warfare—conventional force-on-force, hide-and-seek, and mud—will have fundamentally different requirements of the Grid. In making this point, this chapter reviews work toward the Grid, projects a linear Grid on the basis of current trends, examines broader requirements of other types of conflict, and concludes by calling for a truly open Grid.

Prospects for the Grid

Progress toward exploiting precision is a harbinger of the Grid's emergence. By the time U.S. forces conducted strike operations in Bosnia, many of the barriers to precision operations observed in the Gulf War had been rectified. PGMs were in greater supply, and aircraft had the guidance equipment they lacked earlier, such as laser- and IR-targeting pods.[2] Interoperability, another problem in the Gulf War, was better. According to Lieutenant General Van Riper, USMC, the greatest advances in command and control came through integrating the many diverse C^3I systems. Integration is facilitating joint communications. Institutional barriers that separate intelligence from operations are dissolving.[3] Imagery from the Predator UAV went directly into military headquarters without being routed through cumbersome intelligence links.

Experiments

One focus of the DOD is on experiments to develop and demonstrate new operational concepts linked to efficiencies from widespread networking. Two experiments in particular, the Army's Task Force (TF) XXI and the Navy's Cooperative Engagement Capability, testify to the U.S. military's eagerness to adapt to the opportunities that technology offers. They also illustrate the conceptual limitations within which adaptiveness is pursued.

The purpose of TF XXI is to get tactical information into the hands of the soldier by automatically generating and distributing battlefield information, orders, and related message traffic. Its heart is the Appliqué, a computer terminal put in every vehicle (dismounted versions are being explored) that offers soldiers a constantly populated map of the battlefield and periodic updates of assignments, logistics, and ambient factors (such as the weather). The Appliqué and its servers are linked by a tactical Internet capable of covering a thousand-plus users (per brigade) in constantly shifting topologies (there are roughly three routers for every four terminals). In March 1997, the Army's Experimental Force (the 1st Brigade of the 4th Infantry Division) went to the National Training Center to see what difference its new configuration might make. It lost (as everyone does there), but its performance demonstrated that internetting can cut the

time required to plan and conduct operations by half; it takes a lot of sensors (and automated sensor-to-database links) to stay current with enemy dispositions; but forcing others to gaze skyward for UAVs quickly tires them.[4]

The Navy CEC was designed to counter the air threat (especially from cruise missiles), especially when ships are operating in littoral waters. Previously, each ship's radar would build incoming missile tracks on the basis of what it alone saw. CEC lets each radar provide semiprocessed data to every other ship, supports a common data fusion algorithm, and creates a consolidated track. Data exchange permits a reduction in dimensional inaccuracies; more frequent data acquisition; sharper beam focusing; earlier alerting; and common ways to identify friends and foes. Passing tracks around to other ships permits one ship to engage a target on the basis of what other ships see. Undergirding CEC is a robust communications system with improvement of several orders of magnitude in bandwidth and electronic countermeasures.

The similarities between CEC and TF XXI are telling. Both programs were accelerated after impressive demonstrations to the Defense Secretary. Both seek operational improvements through improved command and control. Both exist, in part, to systematize advantages offered by GPS. And both cost in the low billions—with the bulk of the money used for better communications hardware. Both TF XXI and CEC reinforce the command paradigm of their owners. The Army widened its net but still gives soldiers what they supposedly need to know.[5] The Navy deepened its net by reinforcing the position of the capital ship—to support the conduct of the battle by traditional means.

The Air Force is examining prospects for global mission planning. In the Gulf War it took 2 full days to rewrite an air tasking order (ATO); the goal is to rewrite it even after aircraft have taken off.[6] Other experiments are under way to deliver satellite information directly to the cockpit of an F-16 and to fuse information gathered by its four tactical intelligence aircraft—AWACS, JSTARS (which once had trouble talking to any unit without a special trailer), Rivet Joint, and Cobra Ball. The Air Force claims that it could then see everything within 400 kilometers of the front line.[7]

Sharing Information

It is not yet clear how deeply tomorrow's military will be networked. DOD strategic internets, together with its nascent Global Broadcasting System, will link commanders wherever they are to battlespace information and planning tools. Atop this network is a growing suite of applications known as the Global Command and Control System (GCCS) and its logistics counterpart, the Global Combat Support System. A key GCCS application is to build the COP. Feed comes from reporting units and sensors using TADIL (a common tactical digital information link), and a universal communications processor formats these data in standard (Navy-derived) ways. After some simple correlation tests,[8] the data are posted to a track-management system (TMS) that a joint mapping toolkit (JMTK) draws from to fill a map for users. In some cases, track data are linked to static or real-time imagery (automatic association of Blue units with their logistics data is still to come). The GCCS common operational picture (COP) may come to provide warfighters with the illumination they need to fight from, but the current system serves only commanders in chief (CINCs) and major reporting commands. The system still lacks the real-time features, resolution,[9] or sensor-processing capability to support operators, much less automatic weaponeering.

As bandwidth widens, aircraft pilots and ship commanders will get more information. In Bosnia, headquarters are richly supplied with data,[10] but information available below the division level to ground units is not appreciably greater than 20 years ago.[11] Much of the best equipment is either too expensive or too heavy[12] for mobile field use.

The United States continues to give allies ever more information.[13] The Army is taking pains to ensure that its battlefield digitization will not leave advanced NATO partners and Japan too far behind. DOD has found that if allies are to cooperate on theater missile defense, they must get immediate data on missile firings from early-warning satellites that once were overly sensitive. Apart from NATO systems, intelligence sharing with allies and coalition partners is ad hoc and piecemeal.

New Doctrine

Doctrine is beginning to reflect the benefits and requirements of illumination. Before the Gulf War, few airmen would have accepted, much less applauded, replacing manned aircraft with UAVs. Not only has the Air Combat Command formed its first UAV squadron, but it has also sought and won tactical control of all UAVs in the theater. Even though Bosnia is more overcast than the Persian Gulf, UAVs were used more aggressively there. Their number and roles will only increase.

As noted, the U.S. Marine Corps and the Army are investigating ways to generate the same firepower from smaller forces supported by standoff fire support. Army officers now talk of "massing fires rather than forces" on tomorrow's nonlinear battlefield.[14]

Consensus is building on the importance of completing military operations quickly (or forgoing them). The ability to transmit plans, assessments, and orders more rapidly has proved valuable in shortening the cycles of planning and operations. To defeat Scuds, which take 4 minutes to set up and fire, at their source, the United States must operate within that cycle; thus, the "2-minute" drill takes on literal meaning. Some see rapid reaction as just as important to future warfighting as the machine gun was to World War I.[15]

The DOD image of conventional conflict 20 years hence can be described as follows:

> *In support of AWACS and JSTARS, high-flying and stealthy UAVs oversee the battlefield, relaying interesting imagery (optical or SAR) to the command center. Bolstered by IR and electronic intelligence, analysts in fusion centers translate readings into targets. Moving targets are posted to long-range attack aircraft, and others to long-range missiles. Where discrimination is difficult or the risk of collateral damage is high, small mobile teams supply the final go/no-go decision. After standoff strikes disorient and decimate foes, larger maneuver teams rush in to put foes to flight and occupy important terrain. In this way, an RMA would emerge from a combination of information dominance,[16] precision strike, and maneuver warfare, all supported by the Grid.*

The Linear Grid

The defense establishment is good at analyzing knowable threats, determining their characteristics, devising countermeasures, and integrating them into other systems. It can solve the known-unknown problem. Large, complex systems often contain assumptions about the nature of and responses to the challenges they were built for, rather than see today's circumstances as just one among many possibilities that must be considered. As designed today, the Grid would reinforce the existing breakdown of defense problems into a set of specific tasks and a bounded requirement for data to feed these tasks. Strategy-to-task breakdowns are popular, because they help cope with complexity, facilitate operational testing, and reflect how today's military subcommunities define themselves.

A Grid that supports rather than transforms the way conventional war is fought would reflect such breakdowns. COP would reflect data collected by complex, unitary[17] sensors either tasked by commanders or set on a preplanned course. The data could be laid atop a common map but are not likely to be fused further; users would see it displayed one way, regardless of context. Whatever further data processing takes place will come from data table manipulations or complex algorithms engineered in advance. Only command centers, not field units, would have access to large flows of information. Coordination across echelons, the services or allies would probably be ad hoc rather than automatic. This would hold also for the flow of news. Information would be there for those who know where to look.

The use of commercial sensors, processors, and nodes in quantity (to perform better in the aggregate and to overcome enemy-induced failures) and networked by software (to realize synergies from numbers) is less likely.[18] Warriors and supplies may be dispersed to reduce vulnerability to WMD. Techniques to disperse ground command centers (which have copious electronic emanations) lag. Few weapons will be able to fly to a moving spot on the map, until image-acquired targets can be geolocated in real time better.

Intelligence will continue to prepare the battlespace but not rule it. Continual[19] coverage and sensor-to-weapon intelligence are needed before the U.S. cycle (to spot, identify, and classify a target, assign it to a platform, engage the weapon, and hit the target) can

reliably beat a foe's ability to emerge from cover, fire and move, and return to cover.

The integration of ground with air sensors will probably lag. Automatic data-fusion systems or the correlation of data across domains may be stalled by the persistence of stovepipe systems (which tightly couple sensors, processing, and displays into a tailored package). Jointness has benefitted from verbal support, ostensible progress, and occasional triumphs (an example is truly joint systems for airborne reconnaissance and theater missile defense). But so long as the services train, buy, and supply things as services, a truly joint Grid will be a long time coming.

A linear Grid would be better than what exists today or what other nations enjoy, but whether it is good enough depends on who it must be used against.[20] It will do if putative foes resemble the Iraq of *Desert Storm*,[21] field assets and use doctrines handed down from the Soviet Union (and are thus easy to recognize), fight wars as organized engagements[22] in fairly open terrain (plains, woods, dry mountains), lack the long-range sensors and weapons to strike assets at a 200-kilometer remove (JSTARS, Aegis, LEO satellites), or lack enough medium-range weapons to saturate U.S. ground defenses.

But as chapter 1 argues, new, sophisticated foes may make good use of the information revolution. They could disperse military forces, move without leaving footprints, learn to operate effectively in dense environments, and use commercial items (as is or slightly modified) instead of military items (and develop software to do so intelligently). If so, U.S. forces might acquire information but might not understand what they see. If adversaries can hit expensive sensor platforms, the United States might be unexpectedly blinded. An adversary that brandishes WMD may inhibit U.S. forces from showing up at all.

So what world[23] *should* the Grid be designed for? At the least, some placeholder should be kept for the possibility that the United States may face a foe as large as what a rich China,[24] a resurgent revanchist Russia, or a lucky and obstreperous India might represent. It should also be designed against foes who master *nasty* technologies (cheap RMAs, WMD, or challenges to air, sea, information, or space lines of communication), or for *messy* chaos such as from global warming, bioenvironmental collapse, or a new anti-Western

ideology). Conflict may also arise from stress caused by shifts in global power from such forces as demographic disparities between a birth surplus in the South and a dearth in the West,[25] revolutions in microtechnologies (electronics, biotechnology, microelectro-mechanical systems) and rapid economic growth in East Asia. Beneath Asia's prosperity lies the sort of rising powers and nationalism seen in peaceful Europe 100 years ago.

Little of this matters if the Grid can be adapted in time, but the unexpected may be overlooked or misunderstood as it builds or even emerges. Features engineered into a system decades back can resist easy eradication, such as the Year 2000 problem. If nothing else, the Grid's designers must take into account the contrarian nature of war. Rigidity in its construction will create weaknesses against which foes can concentrate efforts.

And for what war? One way of illustrating how wide the Grid's span should be is to note some key distinctions among traditional combat, standoff operations, and mud warfare:

- In traditional combat, targets and their locations are generally known, and the problem is effective application of force. Standoff operations deal with known unknowns: targets are known but not their locations. In mud warfare, neither the target nor its location is known; at best, one can sense what is normal but not an emerging threat to what is normal. Often, enemy operations must be inferred from anomalies in an environment.
- In traditional combat, an ideal is to deliver imagery data from complex sensors to warfighters. Standoff operations call for the ability to scan large areas and find and identify targets, a need that puts a premium on quick conversion of data to information that will inform action. (As an example, once a Scud launcher is seen, it becomes a target; immediate intention is irrelevant.) Mud warfare requires warfighters to understand their environment intimately; it stresses the recognition of patterns and similar epiphenomena.
- In traditional combat, complexity arises from the imperative to coordinate large agglomerations (such as the Army's ability to maneuver in full corps, or the Air Force's ability to generate a full

air tasking order (ATO). In standoff operations, gathering and organizing information are complex; operations are generally easier to undertake than in traditional situations.[26] In mud warfare the environment, and thus a nuanced understanding of it, are complex.

- What faster speed can buy will vary with the environment of a conflict. Traditionally, fast response times mean being able to act faster than foes can respond.[27] In standoff operations, the ability to strike evanescent targets is what matters. In the mud environment, a faster cycle time permits forces to control a situation just prior to its descent into chaos or dissipation.[28]

The Grid helps commanders to see and grasp a complicated mix of friendly and hostile forces, in part by using the celebrated "directed telescope" to focus on key features of the battlespace. The classic crowded battlefield, however, is obsolete[29] if both sides have sensors; staying hidden is more important. Engagements are intermittent (often a result of mistakes), and any one of them could grab a commander's attention; command authority comes from having the big picture (often literally so). In mud warfare, where power is concentrated against congealing chaos, it makes sense to organize in squads (12 warriors) for patrol and companies (20 squads) for concentration, with only a thin hierarchy above (much as modern factories are organized). These distinctions are summarized in table 3.

The United States may just as well build a Grid that can, among other things, master standoff war and thereby put to bed just the thought of provoking conventional warfare. But designing a Grid that cannot cope with mud warfare would be an invitation to engage the United States where it is least prepared. U.S. forces may not spend all that much time in the mud (at least, not en masse) but it would be useful to develop C^4ISR systems that would allow those so engaged to do so effectively and safely. One need not believe in the efficacy of guerrilla warfare to argue that the conflict the United States needs to be prepared to fight could rage over a wide area, amongst clutter and confusion, against unpredictable foes, and under a heavy barrage of information warfare (broadly defined).

TABLE 3. *Characterizing types of conflict*

	Traditional	*Standoff*	*Mud*
Environment	Known	Known unknown	Unknown unknown
Goal	Data	Information	Understanding
Complexity	Operations	Finding things	Sensing patterns
Why Speed	Faster cycle time	Fleeting targets	Fleeting control
Command	Mixed	Moves up	Moves down

Victory often goes to the side that learns—thus, learns to change—fastest. Hammers are counterproductive if they persuade their users to see the world as nails.[30] Even in peace, threats and tools evolve, and so does much of how militaries organize themselves to respond. Assumptions buried in systems architectures become increasingly impervious to change. The Grid must be flexible to begin with, and its architecture must be as free as possible of unnecessary assumptions. It is difficult to build systems that are flexible against unknown-unknowns, whether these come from the environment or wily foes. But a serious military has no alternative.

Notes

1. Jacques Gansler, Under Secretary of Defense for Acquisition and Technology, labeled an "integrated, secure, and 'smart' C^{4}ISR infrastructure" as "*the* critical element of an effective 21st century warfighting capability;" speech before the Aerospace Industry Association, November 21, 1997.

2. Robert Holzer, "Allies Use Carrot-and-Stick Tactic in Bosnia," *Defense News*, September 4, 1994, 1.

3. During the Gulf War, it took 3 days to translate intelligence reports of suspicious activity, through channels, into mission assignments for aircraft. Direct phone talks between Rear Admiral McConnell of the Joint Staff and Brigadier General Glosson in Saudi Arabia were required to short-circuit this

process and reduce the turnaround time in order to attack critical targets within 3 hours of detection. See David Fulghum, "Glosson: U.S. Gulf War Shortfalls Linger," *Aviation Week and Space Technology,* January 29, 1996, 58-61.

4. See Sean Naylor, "Mission Accomplished," *Army Times,* April 28, 1997, 12-20.

5. The Army's Force XXI is scheduled to be completed in 2010, which suggests that major changes in its architecture are unlikely until afterward. It envisions battalion tactical operations centers richly provided with information: the All-Source Analysis System for intelligence, the Maneuver Control System for force planning, the Advanced Field Artillery Tactical Data System for force application, and the Warfighter's Associate for tapping into the Battlefield Awareness and Data Dissemination system. But the Appliqué is a passive device useful only for maps and a handful of preformatted messages. The dropoff in capability—thus, the capacity for initiative—between the battalion and the company level is enormous. By hard-wiring into its architecture certain assumptions about where command takes place, the Army may limit its flexibility for pushing initiative downward or interoperating with Marines, who do.

6. During the Gulf War, Air Force air tasking orders were routinely passed manually to Navy aircraft carriers. Rome Laboratories now has an experimental planning system that measures cycles in minutes.

7. See David Fulghum, "Electronic Recon Sparks Battlefield Dominance," *Aviation Week and Space Technology,* June 24, 1996, 53-54.

8. The correlator ensures only that every reference to an item (for example, a unit) with the same name is linked to form a continuous track.

9. Except insofar as contributing sensors, such as those carried by JSTARS or AWACS, generate operationally useful data on their own.

10. Richard Rapaport, "World War 3.1: The Shape of Things to Come?" *Forbes ASAP,* October 7, 1996, 125-132.

11. Kenneth Allard, "Bosnia End-of-Tour Report," memorandum to the President, National Defense University, Washington, August 5, 1996.

12. BADD terminals can weigh 250 kilograms in part because they contain hardened boxes that quickly decrypt individual 53-byte cells in bulk before passing them to recipients.

13. French peacekeeping forces in Bosnia, for instance, used real-time airborne video surveillance to monitor Mostar's polling places, which put them in a position to concentrate their forces against potential disturbances without needing to patrol polls directly. *Improved Application of Intelligence to the Battlefield* (Washington: Department of Defense, Defense Science Board, February 24, 1997), 46.

14. U.S. Army Training and Doctrine Command Pamphlet 525-5, *Force XXI Operations* (Washington: 1994).

15. Bing West, quoted in Jason Glashow, "U.S. Army, Marines to Study Urban Warfare Technology," *Defense News*, May 1, 1995, 18.

16. Information dominance is meaningless in itself, because each side's need for information differs greatly. The real issue is who needs what information to do which tasks and how much of that information it can obtain. The ability to illuminate the physical battlespace, which may predict an enemy's operational moves, offers little insight into what the other side thinks, believes, and wants (and how badly), thus what its strategic plans are. Knowing the enemy remains a quintessentially human act and requires knowing how to think as the enemy does. Paradoxically, the more the U.S. way of war is influenced by its access to technology, the harder it may be for warfighters to understand adversaries that lack such access, but fortunately, adversaries also will have a harder time understanding us.

17. Emitters (which generate the signal, echoes of which are then analyzed) are what make radars visible. Separating cheap emitters from expensive receivers would help protect the latter were the former found and hit. Where a large dish might be spotted, substituting many small ones linked by sophisticated software could provide comparable power. Separated lasers and laser detectors are another example.

18. The defense industry's consolidation into three large firms (Boeing, Lockheed Martin, and Raytheon) has sharply reduced the odds that one company would break ranks and undermine conventional complex systems with unconventional cheap ones. As Mickey Blackwell, head of Lockheed Martin's Aeronautical Sector, argued (in an interview in *Defense News*, February 12, 1996, 38), his company saw little future in a drone "cost[ing] $10,000 apiece. Now when you add sophistication to it, when you add stealth, you add a lot of advanced software imagery and optics; now that is our line of business." If his comments are indicative, networks of cheap devices are more likely to come from beyond the defense sector—later and more disruptively.

19. Although continual coverage does not reduce Blue's cycle time, it permits Blue to respond earlier in Red's cycle.

20. Because "against" implies conflict, this may be the wrong issue for a military designed mainly for peace operations. Such a military, however, is unlikely. Peace operations are little more than a muscular version of foreign aid, a budget item the U.S. public consistently places highest on its "cut" list. How popular would the 1992 Somalia operation have been if President Bush had asked for a 2-cents-per-gallon tax on gasoline to pay for its marginal costs (which assume the forces over there would have been paid

for and fed even if they stayed home)? Organizing DOD to counter terrorists operating inside the United States is untenable because law and custom firmly assign such functions to domestic enforcement authorities.

21. This is not to say that each service wants to fight *Desert Storm* again in exactly the same way—the Air Force sees little reason for anyone to set foot in the war zone, and the Marines are playing with complexity theory for urban conflicts—but the assumed superiority of U.S. forces in force-on-force engagements pervades planning.

22. For an analysis of the canonical invasion (e.g., with 15,000 separate pieces of equipment), see Fred Frostic et al., *The New Calculus* (Santa Monica, CA: The RAND Corporation, 1993).

23. There is no shortage of potential futures from which to choose: Frank Fukuyama, *The End of History* (NY: Free Press, 1992); Samuel P. Huntington, "The Clash of Civilizations?" *Foreign Affairs* 72, 3 (1993), 22-49; Robert D. Kaplan, "The Coming Anarchy," *The Atlantic Monthly* 273, 2 (February 1994), 44-76; Matthew Connelly and Paul Kennedy, "Must It Be the West Against the Rest?" *The Atlantic Monthly,* December 1994, 61-91; and Jim Barber, *Jihad vs. McWorld* (NY: Times Books, 1996). Technology-oriented futures range from the pessimistic musings of cyberpunks to the optimistic ravings of extropians. Ed Regis, "Meet the Extropians," *Wired,* October 1994, 102-108, 149.

24. China as a hostile great power is one—but only one—outcome of Asian economic growth. But China has far to go. Its Army must make profits to cover half its budget. Its published military thought is derivative. See Michael Pillsbury, *Chinese Views of Future Warfare* (Washington: NDU Press, 1997). As of the end of 1996, the Chinese Army had lost three of its last six heavy rocket launches through preventable malfunctions. Even its aspirations are modest: China's military sees the 1991 U.S. military as its goal for 2015. Jason Glashow, "DOD Sees China Molding Doctrine Based on Gulf War," *Defense News,* April 29, 1996, 3. India is in many ways more impressive.

25. With birth rates in underdeveloped countries dropping, the year 2015 is more likely to see an unusually large cohort of hard-to-employ youths rather than a Malthusian disaster. See Patrick Clawson, "Demographic Stresses," in *Project 2015,* ed. Patrick Cronin (Washington: NDU Press, 1996), 55-56. As recently as 1978, the 700 million of Europe were four times as many as their counterparts in the Middle East (Iran plus Arab countries). By 2015, Europe will have just over eight million 22-year-olds; the Middle East, close to nine million.

26. Standoff PGM strikes, for example, usually need less planning than the use of platforms, which require coordination (e.g., for logistics),

deconfliction (keeping them out of one another's way, and adjudicating claims for the same resources), and recovery.

27. The Joint Chief of Staff's *Joint Vision 2010* edges toward a theory of time-based warfare by redefining "maneuver." A foe does not need to be destroyed in detail if its operations can be disrupted by strikes at precisely the right time and place (for example, by dropping the bridge just when the adversary's forces are about to cross it). This theory justifies both nodal warfare and the military relevance of weaponry with temporary effects (nonlethal weapons, antielectronic devices). Or see Doug McGregor, *Breaking the Phalanx* (Westport, CT: Praeger, 1997), 37: "Armed forces execute dominating maneuver when they successfully exploit technology, organization, training, and leadership to attain qualitatively superior fighting power as well as dramatic positional advantages in time and space which the enemy's countermeasures cannot defeat."

28. U.S. forces in Vietnam and Soviet forces in Afghanistan both found it difficult to destroy more than 10 to 20 percent of the guerrillas they encountered before the rest disappeared into the terrain.

29. A large army in action—even coordinated action—may not imply a crowded battlefield if only a few units are fighting at any one time. Hide-and-seek warfare turns bloody only when targets slip up and appear visible.

30. If the Grid were to help U.S. forces engage armor efficiently, antiarmor actions might be considered the essence of combat and everything else peripheral. It is natural to pay attention to easily collectible indicators and disregard those more difficult to obtain. The Vietnam War was a rough lesson in both.

4.
Characteristics

The Internet is only an agglomeration of networks, but it has attributes not necessarily present in any one network. Similarly, the Grid will have attributes that go beyond those of its components. How knowledge is discovered and reconciled, how heterogenous data streams are viewed together, how systems work securely and in synchrony—all are issues that might be solved for each component, but remain unresolved for the Grid as a whole. System issues—at both policy and technological levels—must be considered. Some concern the depth and breadth of C[4]ISR integration. Others concern key Grid functions: knowledge management, presentation, networking, and security.

Defining the Grid

Almost every node[1] in DOD will be connected directly or indirectly. But how deeply they will be linked is another issue. There are four levels of integration: physical, syntactic, semantic, and services. At the physical level, nodes exchange bits, much as fax machines do, adequate enough if people are on both ends of the communication. At the syntactic level, the bits are formatted according to some standard or meta-standard.[2] Nodes can be programmed to respond to other nodes on the basis of formatted bits (such as through database manipulation). At the semantic level, bits are organized into mutually understood referents—words, as it were. This level permits knowledge processing. Integration to the services level permits nodes to express requirements, intentions, capabilities, and ways to negotiate them. The deeper the integration, the more each node can say to one another.[3]

The Grid is both a network and knowledge base, much as light is both wave and particle. As a network, it lets users communicate,

access, and manipulate information, read and command devices, and support activities as complex as distributed collaborative planning. But the Grid is valuable for what it gives users: Blue knowledge (what the DOD owns or works with: the C^3 in C^4ISR), Red knowledge (the ISR in C^4ISR), and Grey knowledge (the environment broadly defined).

Why Integrate?

Integration is not free; it takes time to settle on funding, security, and standards. Costs include hardware (an example is $5 million for a connection to the Navy's CEC) and network software (which may embody potential faults that may compromise the performance of equipment so connected). Security problems often arise from linking systems with different risk profiles and thus habits. Networking requires communications; doing so over the air, however, generates RF energy, which creates a detectable signature. Fights over standards seem petty, but standards often reflect fundamentally different ways of looking at things.[4] The use of standards requires that data flows efficiently expressed in a native tongue be inefficiently expressed for more general communication. But the benefits of integration are real: the ability to illuminate battlespace, exercise all-points command and control, conduct comprehensive planning, and learn lessons collectively.

A battlespace is illuminated by having sensor data fused, processed, and presented to warfighters. Sensor integration can reveal objects that individual sensors neither see nor distinguish. Connectivity permits the automatic provision of real-time information, which, in turn, means sensor data go to shooters in time for them to find and strike fleeting targets. Integration could provide allies with a stream of consolidated illumination. Integration is required when the number of sensors increases beyond what can be managed by hand and so must be managed automatically: each sensor needs to know where to move or point, which frequencies to use, how to report, and what to tell the others sensors to do. A battlespace illuminated for U.S. forces would enable both precision engagement (because targets can be precisely located) and full-dimensional protection (because

opposing shooters and their projectiles can be located)—two of the four pillars of *Joint Vision 2010*.

An integrated Grid could tell commanders the location and working status of all their assets, enabling dominant maneuver, the third pillar of *Joint Vision 2010*. A global network would let a commander reach everyone. Standards and other software hooks will let commanders read the various devices within their purview. But control from afar requires exchanging a large amount of data to support security, continuous reliability, and feedback (for safety[5] and effectiveness). With systemwide connectivity, a battalion ashore could command firepower from ships offshore. An Aegis system on a Navy cruiser could control a battery of Patriot missiles. As the range of weapons lengthens, the number that can strike a target increases, so that more potential actions have to be coordinated and deconflicted from the top down or by mutual give and take.[6]

Comprehensive planning—including scheduling, modeling, rehearsal, simulation, and testing—works best when based on a complete picture of the battlespace (such as Red's dispositions and Blue's plans). Knowledge of what's where is helpful in sending the right stuff (only the right stuff) to the right people. This is focused logistics, the fourth pillar of *Joint Vision 2010*.

Community learning allows the experience of one to improve the understanding of many. The Grid should gather, process, organize, and archive lessons learned. As more facts (notably, results from individual engagements) are gathered into a common analytic perspective, the experience base for reaching conclusions and disseminating them broadens. Correlations, for instance, of electronic emanations and events not initially obvious may become clear on further analysis. For instance, American commanders could not begin to end the threat posed by German submarines to Atlantic coast shipping in early 1942 until they found a systematic way to tell one another what they had discovered through contact with the enemy.[7] The Grid could support real-time learning. Warfighters, looking over one another's shoulders as each taps into the Grid can sense the others' needs and deduce what each may be thinking and planning. Practice can lead to the sort of group knowledge Admiral Nelson's "Band of Brothers" exploited at the Battle of Trafalgar, when each

ship's captain acted knowing what the others were doing even when unable to communicate with them.

What Should be Integrated

At a minimum, networks, data repositories, and essential servers ought to be integrated in real time[8] and stay connected. Some nodes need to pass information automatically to other nodes for knowledge processing; others can or ought to pass information through people. Beyond that lies everything else— sensors, weapons, and junctions to platforms—that may need some real-time linkage; but how much? Consider an Aegis cruiser. Its radar, subsurface, and helicopter sensors could feasibly be linked to the Grid. So could its fire control systems (such as for guns and missiles), if these were tasked remotely (CEC permits one ship to inform but not task another ship's fire control systems).

It may be easier to ask what should *not* be connected. Battlespace illumination allows shooters to select targets from an integrated picture of the battlespace. In some cases, routing sensor data through the Grid and then to a shooter may add too much lead time.[9] A Phalanx gun spots, tracks, and shoots at incoming antiship missiles without human, much less off-ship, intervention (although it may report radar tracks in real time). Air warriors in Colorado cannot win UAV dogfights in the Persian Gulf without farfetched assumptions about the connectivity the Grid supports.

Real-time global connectivity sometimes may not be worth the trouble. A ship's power plant may be wired into its bridge and, in turn, wired into the Grid, but the need for real-time data on power plant performance is scarcely obvious.[10] Focused logistics suggest that equipment may be networked so that off-board experts or expert systems can help maintain it. Although inventories of the ship's contents should enter the Grid, they need not be entered in real time; after all, the ship cannot be resupplied immediately.

Other links may be harmful. Special operations forces or submarines work silently and cannot afford to feed the Grid in real time or depend on its availability. Some operations are so highly classified or sensitive that the slightest risk of compromise outweighs any advantage of automatic connectivity. Barriers between the

command of strategic nuclear systems and other military systems may be necessary for political as well as security reasons.

Issues

Although the Grid will reflect the characteristics of its components, it will also possess attributes that result from solving broad technological and policy issues. Some policy issues echo questions of how integrated DOD wants to become—and how badly. Should differences in perceptions among component commands be suppressed or reconciled to form a single ground truth or should there be many ground truths? The answer determines how information is discovered and made internally consistent. How common should situational awareness be? Ideally, those who log on to the Grid—whether from from a tank, a ship, an aircraft, an instrumented weapon, a command staff, or the White House Situation Room—should be able to get the same newsfeeds, services, and answers. Where data, algorithms, agents, or procedures actually sit should not matter—but it will. Classified data will be restricted to some. Networking constraints may abound. The selective highlighting or filtering of data by users (or their commanders) may cause them to perceive situations in a variety of ways.

The Internet, in particular the World Wide Web, is one model for the Grid. It has many virtues: it exists, it works, and it adds users, information, and services easily. But the Internet has few real-time guarantees, poor security, inadequate discovery tools, haphazard organization, and no obvious way to separate the wheat from the chaff.

The 1996 *Advanced Battlespace Information System*[11] (ABIS) study offers another model. The ABIS would be a globally accessible knowledge base that can be extended quickly from the continental United States to any global theater to support any joint or combined-force package, to respond to planned and unexpected demands of users (who can "craft their own information environments"). It would work with anything else brought to battle—securely, constantly, in the face of information warfare, and with a small footprint. It would be tailored for distributed collaborative planning that spans native heterogeneous systems and presents information in many ways—and

all without hassles.[12] It runs on fat pipes, but where bandwidth is tight, data flows are adjusted in two ways. Methods such as bandwidth reallocation on demand, congestion signalling, or compression are well understood. Others, such as substituting knowledge for data and offering "only enough" information for the mission, lie at the edge of technology.

The study was essentially a collection of desiderata, some more plausible than others.[13] Many inspired Advanced Concept Technology Demonstrations for various purposes: enhancing situational assessment, modeling and simulation, and robust networking. But ABIS was not a policy document and did not address issues, other than research and development, that had to be resolved to build the Grid.

With this and other[14] studies as a baseline, the interplay of policy and technology can be seen in the consideration of several broad issues: knowledge maintenance, presentation, access, and security.

Knowledge Maintenance

If the Grid is to illuminate the battlespace, at some level it must have methods to organize, update, validate, reconcile, discover, and annotate knowledge.

To illuminate the battlespace the Grid must hold a great deal of knowledge: targets recognized and tracked, estimates (the likelihood that a tract may be mined or that certain reports may be trusted), short-term forecasts (traffic patterns five minutes hence), and rules (that enemy doctrine puts three tanks together before a village attack). Targets and tracks laid on a map may be equivalent to a real-time picture of a battlespace, but information can also be laid on dependency charts, trading flows, data tables, simulations, and so on. Exactly what servers hold which knowledge ought to be irrelevant for users but transparent to applications that construct the many tableaux that users may need.

The most obvious organization of information, notably "what's where" information, is a geographical information system, or map. Maps may portray raw sensor output[15] (such as UAV imagery, space-based SAR, F-15 forward-looking IR tracks) and translated symbols (such as Blue and Red forces) placed on quasi-permanent features.[16]

An accurate map updated in real time would certainly be better than what warriors take into battle today, but it is not the holy grail. Sensor data must often be supported by further analysis (automatic target recognition and change detection, pattern inference, fusion). Some relationships cannot be placed on maps very well: if-then rules, interaction patterns, dependence relationships, financial flows, and almost anything in cyberspace. Perishable or uncertain[17] information can be difficult to represent clearly. Geographical data need to be converted to support certain applications.

Information can also be organized by linking estimates to operational plans with their objectives, subtasks, milestones, and contingencies. Map- and plan-based schemas could be used together—as long as how the *organization* of knowledge may affect its *perception*[18] is understood.

Whatever structure holds knowledge must also be able to handle unexpected requirements for tracking new indicators. A quiet area may suddenly burst into crisis. At first, sensors in space are tasked to keep the area under increasing surveillance; human agents are debriefed more frequently. If the crisis grows, UAVs and naval sensors may be added; ground sensors may then be dropped in. Local allies may be put on the Grid. Information previously judged too peripheral to be tracked by the Grid (such as signals intelligence) may be shunted into data-fusion nodes and into more user-alert lists. In contrast, links that keep the battlespace map current may go down (because of destruction, the need for radio silence, or network congestion). When connectivity is restored, requests for resynchronization will surface.

The Grid needs good paths between data and knowledge. Some paths are well understood (images from a meteorological satellite can be fed to a weather database or from a sensor to an earmarked data-fusion engine). Other paths must be built on demand, especially for new estimates ("hey, let's track this"). Sensors working together may, for instance, discover fresh jeep tracks; somewhere in the Grid, connections would need to be found between this new observation and the estimates that might be affected by it. Data could be shot to one of several globally interconnected switchboards and then routed by content. Because estimates lead to inferences, themselves

estimates, mechanisms will be needed for forward notification whenever underlying facts change sufficiently. Data can also be circulated to the right place using bots (wide-area, data-polling agents) or webcasters (real-time news subscriber lists). Software agents[19] could update estimates (to maintain maps, for example) or shuttle raw data to other estimates they may affect.[20] Other agents may generate alerts[21] and newsfeeds.

Agents may play other roles. One type could review formal plans and informal intentions ("I'm going to check this out") to see whether they conform to a commander's intent, the plans of potentially parallel units, or rules of engagement. A user may want several agents, each with a different point of view. With time, experience may determine which advisor is worth listening to. At the global level, successful agents could replicate themselves (or use genetic algorithms to build new agents from parents). Failures would wither. Global agents could test the Grid's rules and assumptions for broad internal consistency and conformance with changing circumstances. Other agents may advertise a new service or database.

The need to find needles of fact in haystacks of data suggests the value of search tools. Users may find random facts in the Grid more easily if their queries, expressed in natural language, were mapped to standard queries to which there are standard responses or links.[22]

Global validation is another concern. A single incident may give rise to many indicators: several people hear a sound, several see a flash, shards are widely distributed. The Grid could collect all inputs; if not forced to compare facts, it could conclude that several incidents have taken place. In a distributed system, facts must be reconciled with one another. One part of the Grid may indicate 100 enemy in a given district, another may indicate 50. Both numbers cannot be right at the same time.[23] Sometimes a single forced estimate is needed; sometimes a user is better off being aware of many estimates.[24]

Because data may be useful but less precise, timely, or reliable than desirable, they ought to come with information on their reliability and methods (facts or algorithms) for authentication.[25] After all, sensors err; analysts, human or automated, may be illogical, self-serving, premature, or simply wrong. Source-based pedigree is one option for both raw and processed estimates. Some estimates may be

countersigned or otherwise vouched for. Command rules must also be authenticated at correct levels. Uncertainty must be correctly presented.[26]

A knowledge base built from data fed by sensors may need human annotation: after-action reports or any other observations. Reportage is often skimpy and spotty, but clarifying and classifying its contents can make it less ambiguous, more systematic, and easier to generalize from, and correlate to extant estimates. Reports could be reviewed for certain phenomena and authors could be queried about information that is absent, inadequately addressed, or ambiguous. A sufficiently sophisticated service could help reports become explicit and complete before being entered into the Grid. Authors would come to understand what they do and do not know.

This example illustrates an important principle of design. The Grid could simply refuse to ingest improperly prepared after-action reports, or it could accept but not certify them, or several certification services, each with different criteria, could each stamp reports (or validate one another's stamps). Other applications (such as reconciling different versions of the same event) could take the different certifications into account when preparing estimates. A commander could call on one or another application when preparing "official" battlefield maps. Greater freedom will bring a greater number of choices but perhaps at the expense of interoperability. A useful compromise might be to let content vary but keep labelling consistent.

Knowledge processing, organization, and access are all problems to which artificial intelligence (AI) has been applied, with varying degrees of success. As AI advances, the sophistication of the Grid will grow, but the Grid should not ride on the hopes of AI's early maturity. Good networking can substitute for AI. Making expertise easier to tap and making information easier to grasp can help users apply their own intelligence to raw and semiprocessed data.

These desiderata may make building the Grid seem unnecessarily difficult, but it should be seen as a long project. Early success is likely in making information accessible through networks and, later, through common formats and common descriptors. Over time, information will become organized. Links among estimates, for updates and

reconciliation, are sparse today but will become denser. The use of rule-based logic, rare today, should also increase.

Presentation

For knowledge to be useful, tools must exist to bring out the right data for the right context and the right user at the right time. The Grid should be able to carry on a mission-oriented dialogue with users, let them display information in ways that best support how they think, and help them summon experts supported by formatted information tableaux. These capabilities arise from a combination of global services (which govern data flows) and local applications (which display them).

A platoon on city patrol, for example, might need to be aware of the character of the neighborhood it patrols, recent events there, those in the crowd likely to threaten the platoon (and under what circumstances), and so on. The platoon may need to unite with counterparts on short notice to present dissuasive force at disputed points. Supporting the platoon might be global information (situational background, commander's intent, weather) and local information (infrastructure conditions, crime reports, the status of local disputes). The natural tendency to ask for everything may lead to overwhelmed users. Some messages should be filtered out and others, such as position location reports, should be converted into database entries. What remains can be sorted by using labels, headers, key words, word clusters, or such criteria as what the unit wants to hear about, what it has been told to watch for, and what its counterparts are doing.

The Grid can, in effect, be an expert. Suppose the platoon sees smoke rising from a building: is it accident, random crime, or hostile activity? Can the platoon handle the situation alone or does it need help? The platoon may report using voice (with audio backup of the sound of the fire), video-clip, or IR image. If the platoon is downwind it could assay the smoke using portable chemical sensors. The Grid would review the building's ownership, potential residents, reports of recent fires, and compensation claims. It may ask the platoon leader to clarify the report by answering questions or having sensors pinged

(those that report only when asked) or double-checked (sensors cannot tell when they misread something).

Conclusions and recommendations may then be generated by expert systems or, better yet, real experts (singly or in collaboration). The expert(s) would be given a well-formatted problem statement, a tableau (a grouping of information on-screen that combines static data and real-time feeds), and perhaps tools to simulate the effects of alternative choices. Responses might include the probable source, cause, and course of the fire, and, with knowledge of mission orders and local rules of engagement, suggestions for action and messages for other units to stand by to help, if warranted. Similar tableaux would permit commanders to give go/no-go decisions on urgent actions.

To maintain a tableau,[27] users could select from a well-rehearsed menu of data, types of maps, or both, explicitly or, as the technology develops, implicitly. Maps with key elements grouped could be continually updated. If all relevant logistics points need to be highlighted, such as warehouses, roads, and chokepoints, the data may already have been generated. Information on the enemy's order of battle—formations, weapons and their ranges, and command nodes—could be displayed along with potential amphibious and air assault sites, etc. Today's modern information displays let users "drill down" from amalgamated surface data to underlaying details and raw information. The trick may be to create a drill-down menu at the same time surface data are requested. Displayed data could be linked in advance to formatted databases: a map of enemy concentrations might be linked to databases of enemy weaponry, which would be linked to intelligence estimates of weapons capability.

Better displays are possible. Heads-up displays may overlay what someone sees (perhaps brightened or polarized) with synthetic inputs: IR, ultraviolet, and millimeter-wave auras, radar reflections, electronic intelligence, perturbations in gravitational and magnetic fields, odors, and pressure gradients. Users could be taught to recognize patterns in such arrangements.

Users ought also to be able to display information as best suits them. Fresh insights may be generated by exploiting rather than overriding a person's tendency to see things differently or hang

information on a different bough of his Christmas tree of cognitive associations.[28] Knowing the user may help the Grid[29] format and frame responses to queries ("what that user wants to know is . . . ") and generate a context for data (through hyperlinks, overlays, or circumscription). When a user asks for "the latest map of the Middle East," the Grid could know how that user defines "Middle East," the level of detail wanted, currency and certainty, the features to present, and the data elements linked to those features. As databases change, the Grid might know when to alert each user, distinguishing what is new from what is really new (which each user can redefine for every context).

Each user could have a display-preference profile. One way to build a profile is by having users select among alternative tableaux or specific features.[30] But users may not know the way they want information arrayed, or their wants may not reflect what they actually need in order to grasp a situation. Alternatively, users may be (1) given simulated situations[31] with alternative information flows and displays, (2) asked to form assessments or make decisions based on that input, (3) graded for performance, and (4) offered a series of flows and displays that lead to progressively better scores. The Grid could play coach[32] by determining whether the users were aware of the relevant information, understood it in their own context, and appreciated its relevance. Practice may even help users construct their own mental trees and test them to learn which ones best reflect battlespace realities (and, often as useful, what information flows users can afford to ignore). The Grid might find that the best presentation varies with each type of problem[33] and each user.

Four notes of caution. First, militaries work as teams whose members must share a situational awareness. If adjusting presentations to each user leads to vastly diverse perceptions, communications within a military might prove difficult ("Did you see that?" "No, that arrangement is not apparent"), and mission planning might be complicated by misinterpretation. Should there be a common presentation style into which individual styles (especially those that permit users to annotate material) can be mapped? Can individual orientations be melded to increase the collective insight while achieving sufficient commonality for effective cooperation?

Should there be a standard way to look at information and, if so, which pieces of information and who will determine them? A ship's commander might set the standard today, but CEC may push the standard up to the Battle Group commander. Should every Air Force pilot be able to design a unique display, or should the joint forces' air combat coordinator mandate one? If the Marine Corps is serious about devolving power down to the squad level, is that where the format will be standardized? These questions go to the heart of the way the services organize themselves.

Second, an unlimited ability to obtain and tailor information may allow users to avoid thinking about what data matter most. In Vietnam, General Donn Starry (a developer of the 1980s Air-Land doctrine) initially thought he needed data on 120 different indicators of conflict. Only 60 could be supported. Deprivation led him to conclude that he got more useful insight from fewer data items. In dealing with intelligence units not under his command, General Starry had to be parsimonious and so had those units report significant changes in only six parameters; this worked even better.[34] A system that allows users to achieve their greatest comfort levels may block information that may test their assumptions.[35] Learning is often a matter of knowing how to drop one mental construct and take up another one.

Third, good displays can be seductive. DARPA is developing ways to generate a three-dimensional "sand table" of cities and other terrain to support operational decisions. Consider its use in evacuating people from a city. The operation may seem easy because planners can imagine having a bird's eye view of the terrain. Then someone walks into the command center with a list of local people who might volunteer to smooth the evacuation. Will this offer be buried by seemingly hard data or get the attention it deserves?

Fourth, the more options a user has, the more complex any presentation software will appear. Tools will be used, maintained, and fed only when understood (a tight link between what the hand does and what the eye sees helps). The Grid has to give users at least an illusion of transparency, but not necessarily invisibility. Knowing why a Grid does what it does is helpful.

Access

The Grid should be able to get information out in many ways; users could ask, or data could be pushed to the user through continuous monitors, tailored newsfeeds and alerts, and e-mail with various levels of priority,[36] or combinations thereof.[37]

Access to applications and local services can be expected to vary by location. Users in the continental United States, thanks to optical fiber, will probably get fatter and faster links. Users remote from fiber, particularly those at sea or in austere locations overseas, will have thinner links to the Grid—but perhaps greater connectivity to nearby sensors and nodes. Although spectrum will constrain throughput (as will limited battery power and the need to limit telltale emissions), DARPA programs such as Global Mobile ought to stretch the limits of reasonable expectations for bandwidth to the field. Emerging AT&T cellular services suggest the feasibility of achieving 128,000 bits per second (bps) to an antenna the size of a mousepad—enough for some image processing and whiteboarding. Metricom's Ricochet system promises 30 to 100,000 bps from very small microcells to laptop computer cards.

Maintaining network performance levels at the tactical level (such as radio communications) under conditions of shot, shell, and electromagnetic interference mandates careful use of bandwidth. It entails network management (rapid reconfiguration, real-time guarantees, bandwidth on demand, intelligent routing) and message management (prioritization and duplication). The Grid ought to offer real-time guarantees to applications that need them or tell them when they cannot get them. Congestion may be managed by having routers ask messages what should be done if they are stuck in traffic.[38] Applications should also have ways to accommodate variations in bandwidth.

At the policy level, managers need tools to distribute privileges so that scarce resources can be applied effectively and help predict how well their part of the Grid handles bit flows and service requirements as it accommodates military users from other domains or, worse, civilian users untrained in how to use the Grid responsibly.

Security

Adversaries will try to attack the Grid by feeding it junk, lies, and viruses. Techniques already exist to cope with such attacks: encryption and authentication, unalterable media for archiving and security, semantic filters to separate core processes from user-access points, continually improved operating systems, the continual testing of nodes, active defenses against intrusions,[39] and vigilance.[40]

As the information environment of the Grid grows more complex (with more and more commercial code), providing security by patching known holes or using firewalls and intrusion detectors will be more difficult. A semantic security model may be needed. After all, although human beings are very complex information-processing systems, most communications among them will not cause them to seize up, cycle endlessly, or flood others with pointless chatter, because people process information at the semantic level, not the bit level, often judge new information in relation to themselves or to particular indicators, and sometimes deduce a speaker's motives for saying it. By analogy to a hedgerow defense, the nodes of the Grid could evaluate *everything* they ingest (even from other Grid nodes) in terms of how they are expected to respond. Nodes could determine whether requests were consistent with former tasking, whether they were inherently reasonable, what the negative consequences of obeying instructions might be (say, cycling or thrashing), whether further guidance or validation should be requested, or whether enough has changed in the world to justify new instructions.[41] Such self-knowledge presupposes that the nodes will work by exchanging information, rather than only in response to commands.

The Grid must be able to cope not only with illicit access but also with licit access gone bad. What if someone in a field unit[42] were given full access to the Grid and was then captured with equipment intact? Data may be encrypted and the equipment may go dead if not reinitialized periodically, but forcing even one prisoner to log onto the Grid could reveal information about all friendly forces. Although the location of Blue forces could be blurred, data on adversary forces would suggest their own visibility and let adversaries test hiding strategies, read what the Grid sees of them, and thereby determine what works. Adversaries inside the system could feed it misleading

information. Keeping users off the Grid because they may be captured may harm morale and solidarity.

Some approaches may limit the size or consequence of the leak. If an enemy is unlikely to be in certain places, access to the Grid could be made contingent on being at the right location.[43] Data in the Grid could grow less accurate over time. Face-to-face authorization could be required for recalibration (but it would increase the risk to remotely operating units). A user under pressure could use a special password (or the Grid could look for patterns of suspicious use that suggest a compromise). Thus alerted, the Grid could withhold sensitive information, introduce errors into data points, and generate new information that looked real but was misleading. It might routinely present information that authorized users are likely to ignore but adversaries might respond to in a tell-tale manner and thus hint at a leak (and if the disinformation were different for each authorized user, locating the source of the leak would be made easier).

Other security problems arise from extending access to untrustworthy partners (e.g., Syrians in the Gulf War, South Vietnamese regulars who proved to be Viet Cong, or otherwise trustworthy Bosnian Muslims with Iranian friends). The inability to transfer information in real time once offered an excuse sufficient to keep partners outside the loop. If the Grid works, that excuse would lose force. At a minimum, certain details can be omitted[44] (for example, maps with lower resolution can be circulated), but existence of omitted details often can be inferred from derived data.

Conclusions

Militaries have historically relied on warfighters to follow orders; enlightened militaries have encouraged them to take initiative in figuring out how. Too often, the information systems that have supported warfighters have made their own assumptions about what they needed to know. The Grid should, instead, let warfighters take the initiative in knowledge as well as action. This entails:

- Maintaining a base of knowledge, which calls for ways to organize existing content, generate derived data from raw data,

route data to the estimates that rest on them, deploy discovery tools, and reconcile and resynchronize the knowledge base

- Adapting information flows to users on the basis of need for their current task, building information tableaux for on-call experts to support decisions, and enhancing what individual users understand of a complex reality
- Keeping users informed through broadcasting, newsfeeds, alerts, and answered questions, supported by networking good enough to keep users blissfully unaware of the chaos at the bit level while their services proceed transparently
- Ensuring the security of a widely accessible Grid by using tools such as anti-intrusion devices, semantic barriers, node-based anomaly detectors, and ways to handle suspect recipients.

Notes

1. At the graphical level, Grids are made of links and nodes—sensors, processors, knowledge bases, devices and so on. As a logical construct, a node can consist of many items. Or, many nodes, each logically but not physically separate, can be found on a single item.

2. A meta-standard is a standard way to describe a format. Standard generalized markup language, the grammar behind the more familiar hypertext markup language, is a meta-standard.

3. Consider an analogy to human development. Babies are born knowing how to make sounds (physical connectivity). In the first few months, they learn how sounds do things (syntactic connectivity). Toddlers learn speech (semantic connectivity). As children mature they learn the social context of conversation (services connectivity).

4. As an example, C++ and Ada seem merely two different ways to write the same thoughts in computer code, but each reflects assumptions about power. C++ makes programs easy to write so that programmers can sleep with the muses. Ada makes bad programs hard to write in order to limit errors and let managers sleep at night. For these and other examples, see Martin C. Libicki, *Information Technology Standards: Quest for the Common Byte* (Boston, MA: Digital Press, 1995). Ken Allard, *Command, Control and the Common Defense* (Washington: NDU Press, 1996), shows that differences in the ways the Navy and the Air Force used aircraft complicated setting standards for the Joint Tactical Information Display System.

5. Safety is an important consideration if weapons can fire suddenly, without adequate precaution, especially if no one anticipates their going off.

6. In the absence of a top-down target allocation, a Grid could help potential shooters announce their intentions, broadcast "I got it," and listen for a good reason why they should not engage (the target is wrong or someone else has it).

7. See Eliot A. Cohen and John Gooch, *Military Misfortunes* (New York: Free Press, 1990), especially "Failure to Learn: American Antisubmarine Warfare in 1942," 59-94.

8. "Real time" varies by mission. For automated operations, feedback and intelligence may have to be current to within fractions of seconds. Operations with people (such as a covering action on a city street) have real-time requirements measurable in seconds. Real time for planning functions may be measured in minutes; for learning, hours may be enough.

9. Packet switching slows messages. Every switch must copy, verify, schedule, and retransmit every packet it receives, and some switches become congested. If the inevitable ATM fabric for the Internet is built, a voice-grade connection may be established for urgent messages. Until terrestrial fiber or low-earth relay communications satellites are ubiquitous near war zones, most messages to the continental United States must be bounced off geosynchronous satellites, adding at least a quarter-second to the trip.

10. There may actually be good reasons to connect normally autonomous systems to the Grid. The engine's designers ashore may want a quick analysis of its performance in order to tweak the next power plant. The Navy's community of power plant operators may learn from one another's experience or want to be wired into expert advice on shore. The controller of an automatic power plant may require real-time access to external software to assay its fuel (external software can be updated automatically and frequently).

11. Co-sponsored by the Director, Defense Research and Engineering, and the Directorate for C^4I (J-6), Joint Staff. See www.dtic.mil/dstp/DSTP/abis/ directory.

12. All systems, including ABIS and the Grid, face a tradeoff between the latest features and the reliability that comes from maturity and experience.

13. Many desiderata—the ability to anticipate enemy moves automatically, find "critical nodes in the adversary's war plans," interpret context, correlate events across domains, resolve ambiguity—require heroic advances in artificial intelligence. Unfortunately, some authors felt impelled to devise benchmarks for their desiderata, many of which cannot be measured or vary greatly from one context to another.

14. See the National Research Council's Computer Science and Telecommunications Board, *Computing and Communications in the Extreme* (Washington: National Academy Press, 1996), especially chapter one and the

discussion of emergency information management (81-91), and Box 3.2, on suggested research (104-105). See also "Information Technology and *Information Applications,*" in *New World Vistas: Air and Space Power for the 21st Century,* U.S. Air Force Scientific Advisory Board (Washington: Government Printing Office, 1995).

15. The technology needed to lay an image precisely on a map in real time (for example, to track a target by reference to absolute coordinates) needs work.

16. DARPA officials envision a Dynamic Database that will orient various sensor inputs atop one geospatial background. David Fulghum, "DARPA Looks Anew at Hidden Targets," *Aviation Week and Space Technology,* January 6, 1997, 56.

17. Some doubtful information can easily be presented (a gray rather than black icon, a blob rather than a point) but not all—particularly when two doubtful statements are linked: this is either here or it is there.

18. For instance, map-based organization makes it easy to be reactive: enemy pops up here, and must be dealt with. Time-based organization makes it easy to be active: the enemy is perceived as an obstacle to completing a task on time. Which view is right depends on how conflict is fought.

19. An agent is a guest-generated code that runs on a host machine (often to access its information). A "travel agent" could circulate among the Web sites of airlines, hotels, and restaurants to look for fleeting bargains and building a package to fit its owner's itinerary.

In theory, anything an agent can do (in a public system) can also be done by passing information back to the guest machine, but the use of agents can reduce the load on the network. Any sufficiently large or open Grid is unfortunately liable to contain rogue or dumb agents. A host machine should be able to be able to partition resources to an agent and, if the need arose, shut down errant agents. Alternatively, the Grid could maintain a list of authorized procedures; to pass an agent to a host machine would be to give it structured data (such as the user's destination, resources, preferences, travel partners) plus pointers to authorized, and thus safe, programs with which to manipulate them.

20. To use a metaphor from biology, an agent may wander among nodes that have receptors for various kinds of data (names of engineers with a particular specialty, requests by them for certain compounds, evidence of their travel). A match stimulates the agent to emit signals that stimulate other agents to activity (reducing certainty thresholds for drawing conclusions or for using a particular variable as a predictive factor) or inhibit them (increasing the thresholds).

21. A cascade of status alerts may follow an event. News that a pilot has been shot down, for example, may affect the need to collect intelligence, liaison with friendlies behind the lines, channel allocation for the pilot's signals, the preparation for search, rescue, and medical treatment, the establishment of stay-away zones for certain operations, and so on. Some second-order effects need to follow automatically (for example, telling rescue teams substances to which the pilot is allergic).

22. S. Whitehead, "Auto-FAQ: An Experiment in Population Leveraging," proceedings of the 2nd International WWW Conference (1994), 25-38.

23. If the separate estimates of 50 and 100 enemy were made at different times, the reconciliation process would have to judge whether such a large shift were possible in such a short time (in which case both estimates could be correct). Reconciliation could be automated, but until AI works as advertised, a more feasible goal is to bring all data together for human evaluation. Such tasks underscore the value of keeping analysts wired into the Grid to make rapid determinations when necessary.

24. A Grid built by federating military service subsystems may host separately derived estimates of the same phenomenon. Even when a single, authorized consolidation method to reconcile estimates is impolitic, user-based applications or agents may form judgments and reconcile estimates on their own. Nevertheless, to do this they must know what estimates lie in the Grid.

25. Nodes conceivably could rate their own validity if there were a single knowledge engine, because data would lead to the same conclusion, regardless of who held it (every CEC node, for instance, uses the same Kalman filter for the same data). In practice, one may want agents to view data differently. In a federated system (especially if supplied by data from many national systems) not every node is equally reliable. Receiving nodes with information that can confirm or contradict what they are sent might ascertain the quality of the information faster than it would take to forward the entire information base to the sender node for similar analysis.

26. There are many ways to process uncertain information: the Polya method, used by George Polya, *Patterns of Plausible Inference* (Princeton: Princeton University Press, 1954); the Dempster-Shafer method, used by George Shafer, *A Mathematical Theory of Evidence* (Princeton: Princeton University Press, 1978); fuzzy logic, used by Lotfi Zadeh et al., *Fuzzy Sets and Their Applications to Cognitive and Decision Processes* (New York: Academic Press, 1975; and Bayesian logic, to name four. Uncertainty comes in many forms: an estimate that is accurate to 5 percent is not the same as a estimate likely to be precise if true but otherwise completely false.

27. "Hostage Rescue in Islandia," an 18-minute DARPA-funded film (Naval Command, Control, and Ocean Surveillance Center, Research, Development, Test, and Evaluation Division) shows how maps, linked databases, message traffic, and hyperlinks can be thrown up seemingly at will in an operational planning session.

28. To cite Ramana Rao et al., "Rich Interaction in the Digital Library," *Communications of the Association for Computing Machinery* 38, 4 (March 1995): 33: "People working in an office make use of a rich set of visual and physical cues when arranging and seeking information . . . representing information about collections and their contained items—so-called meta-information—is needed not just to support integration across disparate sources and services, but just as importantly, to support a number of other activities . . . including selecting, understanding, utilizing, and remembering sources and their contents."

29. Presentation is a matter of the Grid supplying the right data and the user's access device displaying them in the right way but the division of labor between the Grid and an access device may vary. Ample bandwidth allows everything to be sent while the device filters what is important. Or the Grid could maintain a user presentation profile and forward it to an access device on login.

30. Flow variables include the messages called or the hyperlinks traversed. Display variables to fiddle with could include how to represent maps (orientation, dimension), time, dependency relationships, and inferred values; how to highlight critical detail; and how to integrate sound and sight.

31. A display that emphasizes certain features in normal times may need to emphasize other features in crisis (for example, in a fire, it is important to know what materials flow in adjacent pipes). Critical as well as common scenarios will need to be tested. Some users may need to be tested when stressed, rather than when relaxed.

32. Of course, if the service is pointless and annoying (such as, today's word processing grammar checkers) users may just turn it off.

33. Consider a beach that rises into the hills behind which lie enemy forces; how risky would a landing be there? A two-dimensional map (even with topographic lines) suggests the enemy is close, so landing appears risky; a three-dimensional map portrays the enemy over the hill, thus less dangerous. The value of the assessment depends on the enemy's sensors and weaponry. If the enemy must see the beach to oppose the landing, then the three-dimensional map will indicate the risks better; if the enemy can see and shoot over the hill, then the two-dimensional map is more useful.

34. Jean-Philippe Dauvin, chief economist for chipmaker SGS-Thomson Microelectronics and reportedly the best forecaster of semiconductor

business cycles, argued that most other forecasters are drowning in statistics. His models consist of a few equations that can be solved with a hand calculator. See Gail Edmondson, "Good Eye, Mr. Chips," *Business Week*, September 8, 1997, 132-133.

35. General Van Riper, who ran the USMC Concept Development Center, has argued that knowing everything about the battlefield is a hopeless quest. Marines, he believes, should be trained to make correct decisions with as little information as possible.

36. How (and by whom) are message priorities determined? Some may automatically flash high. Others will be rated by senders or third-party raters. Yet when everyone shouts, no one is heard. Users ought to be able to adjust these ratings (and filter messages accordingly) by rating the rater's credibility.

37. A guided-tour presentation may have the user ask for a general subject area and then given the equivalent of a Web site, with content filled in as the Grid perceives the implicit focus of the user.

38. Consider what happens when an e-mail stating the recipient is on vacation is received by someone that automatically responds with similar news.

39. Analogies to the human immune system ought to be treated with caution. Even though tomorrow's information environment may be infected with hostile agents, knock-knock bots, and virus-laden sirens, relying on automatic responses to specific invasions might push foes to find ways to induce a cyber equivalent of anaphylactic shock.

40. A well-secured system invariably includes human checks and balances and is manned by those who can spot anomalies and have practiced recovery schemes for systemic, accidental, and induced faults. A security regime for the Grid may resemble today's network management monitors: it would scan itself periodically and filter strange events up to experts looking at a rich tableau of system parameters.

41. Compare this to the three rules found in Isaac Asimov, *Robot* (New York: Doubleday, 1950), 11: (1) A robot may not injure a human being, or, through inaction, allow a human being to come to harm. (2) A robot must obey the orders given it by human beings except where such orders would conflict with the First Law. (3) A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

42. The Grid can leak because of traitors. Discovering them and neutralizing their effects is more difficult than controlling the damage wreaked by suborned prisoners. Preventing the contents of a display from being retransmitted can limit how badly the Grid leaks but will not prevent leaks. Searching for suspicious access patterns (e.g., queries that suggest

espionage) may indicate that a traitor is operating.

43. To defeat an enemy's feeding false GPS signals, each display could have a sealed GPS receiver, which would sign and thus authenticate its location, and each satellite could sign and time-stamp transmissions, to inhibit spoofing or echoing. Or, terminals could respond only to weak local signals.

44. An example is the Multi-Level Secure Releasability Server from DEC, Planning Research Corporation, and Oracle. See Pat Cooper, "Military to Test Intelligence Delivery System," *Defense News,* August 28, 1995, 12.

5.
Construction

If DOD managed the Grid's creation as it does other defense programs, the path from concept to implementation would be a series of steps: designating a program office, establishing requirements, selecting contractors to do the work, writing and testing code, evaluating the final product, then fielding it.

Creating the Grid calls for different steps if only because of the Grid's size and complexity, and because integration is not construction. DOD needs consensus on a broad vision for the Grid (see chapter 4). It must establish core services, standards for interconnection and interoperability, and methods that let nodes integrate themselves quickly under both normal and wartime conditions, and then hang new nodes and services on the structure so created. In the process of creation, the Grid could become the world's largest testbed for new information technologies.

To address issues involved in its creation, this chapter points out some difficulties of top-down integration: a process that encompasses a requirements definition, a hierarchical decomposition of tasks, and the specification of hardware and software to meet these tasks under central control. Next are examined some prospects for bottom-up integration: where systems, subsystems, and components are given much more leeway in meeting broad goals through their own resources and help negotiated with their peers. Then the role of architecture is discussed, and guidelines for planning, experimentation and R&D suggested.

Some Difficulties of Top-Down Integration

As a top-down project, the creation of the Grid could be the single largest software project ever attempted. Great size makes any project difficult to manage and may lead to results too fragile to field.

Because the Grid must absorb and accommodate existing capabilities, the conventional model of systems integration may not fit.

Great Size

A complete top-down Grid could include every process, application, service, database definition, and interface specification entailed in a complete C[4]ISR system. It may, at the outside, require a billion lines of code costing $5 to $10 billion a year for a decade or two.[1] Software accounts for a growing share of a defense system's costs, and integration is a growing share of the cost of software. A large program, such as the F-22 fighter, may include $5 to $10 billion worth of systems integration (some of that is to ensure that hardware can fit in tight spaces and work together reliably). The next-generation Air traffic control system had, by mid-1997, absorbed $7.6 billion, mostly for software.[2] Although increasing the connectivity of DOD equipment may not be expensive,[3] a top-down tightly coupled Grid may be. Is something so large doable?

Finding money may be a problem. Only the services can raise so much money and only if working together. Dividing the Grid into modules, tasking each to a service, and reintegrating their results could take whatever time was required to build the modules, plus years of politics to the front for apportionment and years of politics to the back for reintegration. Even then, the services might not want to spend billions on a top-down design not of their own making. No service would relinquish its oversight over the Grid's development once it sees how much design decisions will influence its own acquisitions. Many are already building their own version of the Grid: the Army Force XXI, the Navy CEC,[4] the DISA GCCS, various ACTDs under DARPA, and the emerging Total Asset Visibility program for logistics, all of which offer the prospect of partial integration at the risk of making complete integration more difficult (with domain-level stovepipes replacing service stovepipes).

Meeting objectives on time and under budget is always a challenge for such a large software project. The difficulty and thus cost of integrating a system grows more quickly than its size. Just as large organizations have many levels from top to bottom, so large integration projects require great coordination between constructs at

the highest level and components at the base. The larger the project, the longer integration will take[5] and the less later contributors will understand of the rationale for early designs.[6] Pressure for early success is great, as is the weight of outside oversight.

Requirements may be impossible to write, much less write concisely.[7] DOD has many constituencies,[8] authority is quite dispersed, and great interests are at stake. The Grid's creation would influence nearly all subsequent defense programs. In-fighting is inevitable, unless a new threat forces everyone to close ranks. The need to test any system against its promises tends to drive contractors to build one that does only what is asked of it and nothing more. As warriors are empowered by information, they will develop operational concepts to change what they need, thus changing what the Grid should provide.[9] The Grid must adapt to every piece of new equipment (especially the putative shift from a few complex sensors to many simple ones); software capability; concept; threat; and even a change in allies. Thousands of adjustments will be asked for, but a flood of change orders in today's acquisition environment drives costs and litigation.

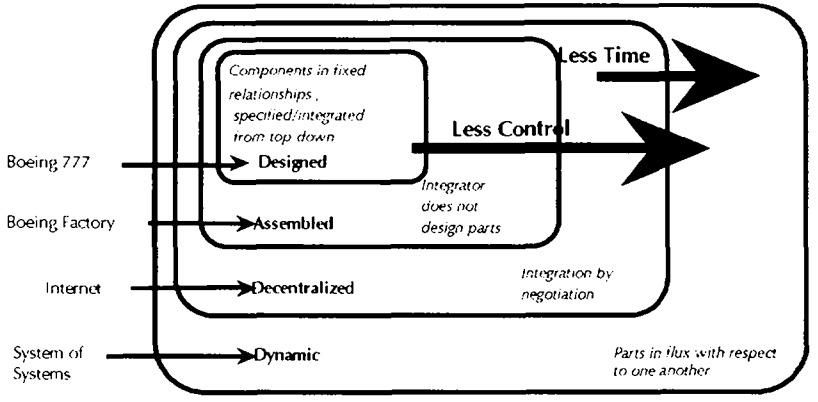
Selecting builders could prove vexing. Perhaps an in-house integrator (a national laboratory or a federally funded research and development center[10]) could oversee the Grid's creation, but that choice is unlikely in the face of today's outsourcing rhetoric. Any one company selected as integrator would thereby gain an incredible edge over all others for all future DOD work. Expecting a team of contractors to work together without each trying to design the Grid that would be to its own later advantage may be wishful thinking.

Models of Systems Integration

Confidence that large systems can be built from the top down by U.S. firms stems from their expertise in solving a particular class of complex integration problems. The Grid, however, will differ from conventional integration problems in both kind and size.[11]

Figure 2 illustrates four systems integration problems by concentric rectangles. The farther out the rectangle, the less discretion an integrator has and the more indirection is needed.

FIGURE 2. ***Integration, four levels***



Designed Systems Integration characterizes the Boeing 777, the Space Shuttle, and similar projects that gave U.S. contractors a reputation for being able to integrate large systems. Such integration occurs when a single integrator connects components that are specified from the top down and related to one another in fixed or predictable ways (e.g., in real space on a ship).[12]

Assembled systems integration involves components built, at best, to standards rather than design. Examples include the relatively straightforward problems of office or factory integration. Integration rests on communications through standard interfaces and results in looser coupling than systems produced through designed systems interface.

Decentralized systems integration eliminates the single integrator. Each subsystem or group of subsystems has its owner. Each owner negotiates with one another over how tasks are allocated or how one subsystem may respond to requirements levied by another subsystem. Examples include the C^2 system cobbled together for Bosnia and, to a certain extent, the Internet itself.

These three models all assume that the relationships among a system's components are static or change slowly—but relationships

among the many components of tomorrow's battlespace are dynamic and unstable: spacecraft zip by; UAVs dart in and out; units move as battle dictates and many take hits; projectiles and sensors appear and disappear. The Grid's components enjoy a stable relationship only before engagement. Even if the enemy did nothing to disturb the laydown of sensors, processors, and users, a Grid will need to reconfigure itself to catch the fleeting opportunities of the battlespace. This capability calls for *dynamic systems integration*.

Cutting to the Core

Integrating the Grid will be easier by isolating domains that can be dealt with without reference to the whole (on the theory that a single billion-dollar problem is less tractable then 10 hundred-million-dollar problems). Three such domains may be information presentation, individual algorithms, and the networking infrastructure. They can be worked independently only if the Grid is open in the sense that no one portion will be able to make blithe assumptions about any other portion (information presentation, network infrastructure).

The way information is presented should reflect what information the Grid holds, but the coupling between information and presentation should be loose enough to permit change in either without also requiring the other to. Because Web mania is an impetus for the development and fielding of user interfaces, DOD can buy most of what it otherwise would need to build.[13]

Many, perhaps most, of the algorithms needed by the Grid address specific military problems: planning deployments, finding specific targets in images, fusing intelligence, optimizing logistics flows, and so on. If algorithms can express their input and output in commonly understood ways,[14] each algorithm (or algorithm domain) could be engineered off-line. Some key applications may place a heavy analytical load on nodes of the Grid. A good user-oriented newsfeed may interact with literally thousands of knowledge bases every time a key piece of information in them changes. Maintaining a detailed real-time map influences what data are collected and how they are organized.

Network infrastructure—devices and protocols—must be considered as a whole. Many challenges in networking the Grid's

nodes resemble those tomorrow's cellular systems will face, but with special requirements for global mobility, security, antijamming, and rapid installation and reconfiguration under stress. Applications, services, and access to data should not need the particulars of the network configuration but only the parameters of its performance.

The core problem of creating the Grid is how to organize and transport data for known algorithms and unknown problems. The process of marshalling data cannot easily be decomposed into modules[15] that can be written and tested separately, because interfaces must cross subsystems and only work if the data transferred are understood by both subsystems. Determining and establishing central services and then getting maximum work from bottom-up integration may be a way to manage the problems of marshalling data. Standards help, but their development takes work,[16] and they alone cannot complete the job.

Opportunities for Bottom-Up Integration

The difference between top-down and bottom-up approaches is where information is processed. In a top-down approach, information flows to a central source, and decisions reflect a global optimum for a particular problem. In a bottom-up approach, individual components reach decisions by using broad rules, detailed knowledge of their own situation, and information they can gather from their environs as well as from negotiations with their neighbors. In theory, a top-down approach can do what a bottom-up algorithm does, if each component sends up all it knows and each request down is expressed by task commands. But for each component to communicate all it knows can be a burden, and the optimization process at the top may be computationally impractical. Such processes may be so difficult to describe algorithmically that once they work, designers or users might hesitate to change them for unexpected circumstances. Although top-down processes tend to be more deterministic, bottom-up approaches are often more robust, especially if situations can be abstracted in generic rather than specific terms to allow components to respond appropriately to possibilities.

One example of a bottom-up approach is the Ethernet in which nodes communicate by sending off a packet and listening for a collision. In a rival architecture, Token Ring, permission to send packets is granted centrally. In Free Flight, the Federal Aviation Administration's proposed air traffic control regime, aircraft find their intercity routes through coordination with one another rather than instruction from control towers. Similar choices can be made in rail transport if boxcars can schedule themselves and use bidding and negotiation to manage the contention for railyard space, rather than have the railyards undergo global allocation. Complexity theorists argue that it is easier to model a flock of birds in flight by programming each bird to adjust its flight path according to where other birds are flying than to generate an individually predetermined flight curve for each bird.

A bottom-up approach relies on coordination of the various pieces, each possessing partial knowledge. A component (a sensor, node, database, controller) recognizes top-down constraints, then uses its understanding of its context (howsoever acquired) and duties, and its rules for responding to contingencies (requests, events) to call on information from other components. In some cases, particularly when many applications compete for the same resources, negotiations among components determine which get what. Similar negotiations mediate the difference between what a task needs and what components can give. Presumably, nodes ask themselves questions similar to what people would in forming organizations: What am I to do? Can I do it on my own? Do I need help? What kind? From whom? How can I contend for resources consistent with expectations for my behavior? Bottom-up approaches make particular sense because the Grid must do the following:

- Absorb the old—the huge DOD investment in existing sensors, weapons systems, networks, and databases).[17] Attaching a translator to the input-output stream of a legacy system may be easier (and more acceptable) than rewriting the software, but it would require stating the demands of the Grid on legacy equipment in sufficiently generic terms to correspond to categories the legacy equipment already uses to process data.

- Accommodate the new. Growth by accretion (the way the Web grows) may allow new sensors, databases, algorithms, and presentation schemes to insert themselves, acquire validation, announce themselves broadly, and link themselves to the most appropriate applications and equipment. Growth in smaller chunks allows more contributors, less program management overhead, and faster feedback. When one component is upgraded in a top-down system, every component that must deal with it must upgrade its software to match. In a bottom-up system, each change would add, at most, only a few words to the common lexicon each node supports.
- Operate in the field despite constraints of spectrum and power. Top-down approaches need more information (sent farther) than bottom-up approaches do. Constant high-power communications make components visible.[18] Bottom-up solutions degrade more gracefully when pieces become disconnected (because of physical destruction and electronic jamming or as a defense against corrupted neighbors). Nodes can remain roughly right even as information input declines.
- Diagnose itself. A bottom-up approach permits administrators to understand the source of a system's (mis)behavior by figuring out how each node (mis)perceived its environment or reacted (poorly) to it. A top-down approach forces the entire process to be examined as a whole.[19]

A Common Tongue

Bottom-up integration requires dialogue so that nodes can negotiate the exchange of needs and data. Dialogue rests on a lexicon for the following:

- Health and status data for network management,[20] including node-specific data
- Messaging plus support for compression, flash status, alerts, and newsfeed filtering
- Addressing and directories that reflect planned as well as past movement and accommodate circuit-switched and continuous links

- Announcing one's existence on the Grid and defining, in general terms, one's purpose and capabilities
- Queries, responses, and meta-responses (e.g., that an answer is incomplete and why)
- References to time, place, and spectrum
- Security, including access, encryption, and authentication
- Meta-standards that indicate what standards a node supports.

Nodes also need words for need-to-know assertions (plus priority and urgency), format negotiations, dialogue markers, and resource constraints. Respondents, as they become more sophisticated, should be able to express and describe the certainty, quality, authenticity, and, perhaps, the rationale for their estimates; contexts in which the answer makes sense;[21] when further clarification would help; and where alternative or complementary sources of data could be found.[22] Respondents should also be able to state intentions, responses to them, assignments, tasking authority, tasking justification, and ways to measure how to complete the task. Nodes should have words to clarify a task and negotiate alternatives to, or variations on, the task if it cannot be completed.

Integrating a Sensor Mesh

A bottom-up approach may help integrate a heterogenous mesh of ground and airborne sensors (see "A World of Sensors," chapter 1).

Coordinating sensors fosters good spatial, spectral, and temporal coverage (lest vision sensors, for example, clump here and acoustic sensors clump there), as well as data fusion. Local coordination is needed whenever bandwidth (even after compression) limits sending everything back to a central source. Processing and in-the-field integration may have to precede out-of-area reporting. To reduce the data flow, sensor readings may have to be preprocessed into microchunks or symbols, that is, by data fusion or by several sensors acting together (just as it takes two eyes to perceive depth). When high-bandwidth devices that receive and transmit are expensive and power-hungry, only a few specially designated sensors need to function also as data nodes.

Sensor meshes need to be organized upon deployment. The vicissitudes of war will put many in the wrong place, pointing the wrong way or unable to obtain good readings. Everyday human activity, not to mention hostile activity, can disturb sensors. Ground sensors also ought to adjust dynamically to airborne sensors such as UAVs. Each sensor might announce its location, where it is looking and over what spectral bands, and its putative assignment (collectors, relays, fusion nodes), and then negotiate for bandwidth. As the battlespace changes, so should the sensor hierarchy. Each sensor may ping others periodically to determine whether and when reassignment is necessary, to elicit the capabilities of its neighbors, and to correlate what neighbors see against what it sees (and inquire further if anomalies are found). Some sensors could be equipped with several capabilities that could be turned on as needed. One pattern of sensors may detect certain phenomena well, while another may be optimized for others. When cued, some sensors might switch parameters or turn certain receptors on and others off. Some sensors may need to turn other sensors on for a closer look and may need to be told when to be silent or when to switch frequencies.

Integrating Knowledge Bases

Ideally, the Grid should allow users to mix and match databases and applications at will. In practice, doing so manually, much less automatically, has long been a problem.[23] A user may know, for instance, that a powerful application (such as a tactical terrain analyzer) is available, but exploiting it requires understanding syntactic conditions. In knowledge bases, similar categories often refer to different definitions, attributes, or assumptions. The term, "production capacity" may presume peacetime or it may presume wartime; it may assume optimized scheduling across factories or just within factories.[24] Databases can routinely trip over spelling. Assumptions useful for understanding what the information implies may be unstated.

Merging models and databases can be slippery. In a shipping model, rates of offloading may assume port space is allocated in order to move the most tonnage per day. A logistics model recognizes that certain equipment can be repaired at, and therefore must be moved

through, certain facilities. Combining the two models cannot yield a prediction of what will happen to the supply of repaired equipment if a port is unavailable or its capacity severely crimped. The shipping model may incorporate slack to accommodate noncombat evacuation, but the mission planning model cannot generate the requisite data.[25]

The persistence of such problems over decades suggests little confidence in quick answers. Standard definitions of specific data elements or general categories of similar characteristics may help integrate models and knowledge bases. Nevertheless, common schema for particular domains may have to be enforced for critical models and databases. Some analytical tools or databases may be so widespread that their interfaces become *de facto* standards and are incorporated into the knowledge base of software agents. As a next-best solution, models and knowledge bases may have standard ways to describe themselves by mapping their categories onto generic schemas.

To make matters worse, real knowledge bases contain unorganized facts and rules[26] and random expertise, all of mixed reliability. Languages, such as knowledge query manipulation language may be needed to turn such chaos into usable information, especially if they let a requestor indicate what constitutes "good enough" and a respondent describe how much it knows.

Combining heterogenous models and knowledge bases may become more tractable if they can somehow be mapped onto a large global generic knowledge base. To bridge language barriers, people often point to and name objects or pantomime actions.[27] Common reference material, like the Web, with its uniform resource locators, can create contexts for certain word and phrases, convey analogies, and provide a basis for testing whether meanings are correctly understood. Language barriers could be bridged by black-box translation: one system sends input to another and then infers the respondent's characteristics by reading what comes back. The Grid may some day interwork with its overseas analogues by exchanging and understanding knowledge bases and applications (such as models, simulations, and agents). International standards will help, but they are not enough.[28]

Some Central Services Are Still Needed

As a network, the Grid needs some centrally planned (though not necessarily centrally administered)[29] services. Examples include switching, addressing (not simple when objects move and routing tables are constantly altered to keep up), directories, and security services (authentication of nodes and agents, infrastructure of public keys, authorization lists). Beyond that, the Grid should be able to do the following:

- Simulate how well it passes bits around to assess its own topology, the readiness of subsections for deployment, and how well specific missions and operational concepts can be supported
- Monitor its own performance at the semantic level (the flow of logic, not just bits) to help detect and delete unwanted behavior (which may emerge from unpredicted interactions, bugs, or security intrusions), manage congestion and contention for common resources,[30] and indicate obsolescent data, rules, and sockets[31]
- Host at least one global content-based discovery service to locate information, determine its currency, and support reconciliation procedures
- Authenticate and prioritize new services and capabilities so that sockets for new tools, tests, and probes can be developed for various knowledge bases
- Manage (and perhaps consolidate) the inevitable proliferation of each user's filter, or alert requests, new services (each advertising itself to user applications), and process-driven flash inflation.

In addition, some services, such as testing the adequacy of battlespace illumination or of operational planning, are so important to warfighting, so joint, and call on so many nodes that they are tantamount to central services.

Architecture

The DOD canonical guide to architecture[32] identifies three types: operational (who says what to whom), systems (the links), and technical (the interface standards).

The value of systems architecture may be exaggerated. Doctrine (plus the expected load from random user requests, algorithms, and management overhead) can suggest how much of the data need flow where, and this estimate can inform the mechanisms that marshall data, but a guess is sufficient. New technology, challenges, and opportunities make the half-life of even a perfect answer short. Tight coupling of doctrine, operational architecture, systems architecture, and software all could make the Grid difficult to change and impede the adaptation of doctrine to varying circumstances.

Ideally, the Grid should let anyone say anything to anyone else at any time. Users scarcely need to get everything at once. But a user-oriented architecture would let users figure out what they need. Their applications would draw from and meld information from whatever servers contain the relevant knowledge bases.

Who the "user" is—every warfighter, only the national command authority, or those in between—will be determined by doctrine. As noted in chapter 3, the Grid can have a centralizing or decentralizing effect, depending on where and how it is used. But doctrine should not fix the Grid, if for no other reason than the Grid will create operational possibilities that lead to new doctrine. Nor should the Grid's architecture make it impossible for any user to enjoy any privilege; restrictions are the job of doctrine. Conversely, the Grid's architecture should not constrain doctrine. DOD needs an architecture that can be easily extended to other nations or other users (civilian agencies, state or local governments, nongovernmental organizations, private voluntary organizations, and support contractors).

The Grid's architecture should let applications determine where they fetch information from, mixing and matching as needed.[33] Nodes should be built in the expectation that they may be tasked from anywhere. Their data structures should be transparent (standard, or at least reasonably self-descriptive) within constraints dictated by who can write to them, and who can read from them.

In the real world, constraints are necessary. Spectrum is limited, congestion plagues links and servers, and applications cannot be rewritten for every point of view. Security considerations and defensive information warfare require that some users have only limited access and others can be shed quickly. Certain time-critical applications cannot realistically mix and match sensors and weapons on the fly, trusting to systemic mechanisms to marshall resources. In some cases, critical information must be pushed to users, regardless of what the users themselves think they need. All these requirements can be addressed by overlaying applications on generic Grid capabilities.

Nevertheless, an open system needs to be consciously sought. A highly adaptive Grid puts a premium on expanding bandwidth, proliferating sensors, establishing a structure of user-oriented newsfeeds and software agents, and transparent knowledge bases.

An Open Grid

If the Grid were open to new data, new uses, and new users, the United States might be able to illuminate the world not just for its own forces but for all. Everyone may profit from knowing that everyone else is being watched. Nasty surprises would be more difficult to hide. Everyone may even come to have a stake in illumination. Alone, the United States (and its friends) could see much. With the complicity of those being watched, much more may be visible.

In essence, respectable nations[34] that make themselves transparent or, better yet, contribute information from their own sensors and monitors, would enjoy access to an opened Grid's services[35] and data. The data would include feeds—video on global flashpoints, the tracks of moving vehicles, the volume of electromagnetic chatter, ambient environmental conditions—indicators—crime reports in a certain neighborhood, local business activity, status updates on humanitarian crises—and monitors—traffic, pollution, network switch activity).[36]

Access to the Grid need not mean sharing all of it with everyone. Data on surface activity would be shared more quickly than data on activity in space (primarily useful for targeting or evading satellites) or

under water. Data might be withheld if their existence suggests which sensitive targets the United States is seeking, if leaking them would make terrorism easier, or if distributing them would frustrate building confidence.

A Rationale for Opening the Grid

Information superiority is now the strong suit of the U.S. military. Giving it away hardly seems an obvious way to maintain power, but doing so wisely may make more sense than pointlessly husbanding a temporary tactical advantage at the expense of a permanent strategic position.

The United States can be aggressively generous without exhausting itself or gaining enmity. As inventor of the Grid, it is likely to take the lead in bringing out successive versions and thus controlling its makeup. Once a structure exists for getting, processing, and transmitting data, other nations—first allies, later unaligned nations—will have a foundation on which they can add their own data and services. They may even work on problems germane to the Grid's functionality. An opened Grid would help the United States offer information to help its friends because compatibility issues would have been worked out beforehand. Everyone's defense systems would work with that of the United States more easily than each would work with those of others.

An opened Grid would still be optimized for what the United States fears most, pass over irrelevances, and look away from U.S. abundance. Buying into the Grid implies buying into these priorities. The easy availability of certain analytical tools, the availability of presentation templates, the differential opportunities for collaboration, and the way knowledge is organized and indexed all influence the way the world is perceived. Others can more easily look for what the United States is looking for and may be frustrated looking for what the United States would avoid highlighting. The Grid would remind others of what can be seen.[37] Although determined countries could work around these tendencies,[38] many would follow the path of least resistance and, over time, willy-nilly acquire more and more of the U.S. orientation.

Uses

An opened Grid not only makes it easier to manage global crises, but it can also support peacekeeping and inhibit arms races. International cooperation is helped if tense situations can be clarified.[39] Flexible responses can be more easily organized because of such consensus. An information umbrella can replace the nuclear umbrella in keeping alliances together. Although international broadcasters may provide a universal perspective, and neutrality adds to their credibility, their data lack validating detail or the broad scope that the Grid could provide. Providing that detail as it is collected limits the criticism that the United States is presenting only a selective or outdated perspective to make a point. With more information about the United States, other nations could feel more assured of its good intentions. Visibility can be considered a valuable instrument of all major powers. A rogue whose misdeeds are broadcast by a Grid fed by everyone would have difficulty directing its ire against the United States alone—or doing so convincingly.

An opened Grid would support peacekeeping. The disengagement and peace agreements of the 1970s that dealt with the Sinai, for example, were reinforced by U.S. sensor systems, which allowed each side to monitor for signs of potential attack. By comparison, wiring the Golan Heights with sensors that feed the Grid could indicate not only impending attack but targeting information—putting trespassers at direct risk.

Global visibility could reduce the tensions that feed arms races. If the opened Grid let every nation clearly see what is coming at them, their confidence in their defenses would be justified. Stability might be further enhanced if all understood that access to such information favored well-behaved nations whose forces were designed for defense. For example, in Asia, where countries formally aligned with the United States still eye one another with suspicion (South Korea and Japan, or Indonesia and Australia), transparency might put old fears to rest without generating new ones.[40]

Consider, as a model, the Incorporated Research Institutions for Seismology coordinated by the U.S. Geophysical Service. A network of thousands of portable instruments run by hundreds of digital stations worldwide monitors seismic events, among them nuclear

tests. In 1986–87, the National Resources Defense Council demonstrated the power of low-cost digital seismometers by installing them near Soviet test sites in cooperation with the Soviet Academy of Sciences:

> [This] showed that a world worried about covert nuclear testing need not rely exclusively on whatever reports the major nuclear nations chose to issue (or not) based on their own, closely held information derived from classified technologies.[41]

Some nations will be wary of growing dependent on an open Grid. Most will want to retain systems of their own. But, in time, as confidence builds in the open Grid, take-or-build decisions would tilt toward taking. Making systems is hard: building and filling them is work, and integrating them is yet more work. Allies will take (rather than make) with grace; others will integrate more slowly and less completely, but given time they may well accede. As they do, their ability or desire to disrupt information flows will diminish. Even a nation with great power ambitions may risk the downside of long-term interdependence for short-term gains in order to:

- Adhere to emerging international norms
- Foster confidence and reassurance
- Support peace operations or other coalitions
- Access tools and databases for managing a nation's space (e.g., environmental, national resources, transportation, law enforcement, and disaster operations)
- Ease entry into the global information infrastructure
- Keep channels open.[42]

The bargain needs to be struck while potential powers are on speaking terms and while the United States enjoys a lead in information technology it can leverage to long-term advantage. Technology may foster global visibility, but international security would be more assured if the United States rather than another power or a private concern[43] should be the one to bring it about.

Planning, Experimentation, and Technology Development

Planning should proceed from vision[44] and milestones, to standards, metrics, and implementation. Standards matter because they are the terms of trade that bind components. They should cover physical connectivity, syntactic connectivity, and, ultimately, semantic connectivity. Metrics are needed to assess the Grid's performance, to determine whether subsystems are ready to be linked to the Grid and to guide decisions on whether to develop or buy technology.

Detailed implementation planning should determine what each component system must do to adapt to the Grid (as the Grid adapts to the load of its populated objects) and in some cases what must be done to make their sensor readings, files, data flows, processes, and output streams globally accessible.[45] Acquisition programs, if young enough, should ensure their products can be linked into the Grid upon fielding. As technology and resources mature, new Grid-wide services can added.

Experimentation

As noted in chapter 3, the services, prompted by the *Quadrennial Defense Review* and encouraged by the National Defense Panel,[46] are experimenting with how to best exploit information technology for warfighting.

Experimentation is important if there is something to be experimented with (or on) to learn whether and where it is useful.[47] A squadron of F-22s may be built, used in simulated combat, altered as necessary, evaluated, and if sufficiently useful, bought in quantity and integrated into the Air Force. For the Grid, "quantity" has little meaning. The Grid must cross some threshold of sophistication to be useful, and growing bigger is less important than growing denser (with sensors, weapons, communications nodes, or workstations).

Adaptation of the Grid to warfighting will probably be continual. No one knows what arrangement of sensors will provide the best battlespace illumination, particularly in the face of cover, concealment, and deception. How widespread networking affects command and control in wartime is still a matter of debate. The

proper mix of artificial and natural intelligence is unclear. Trading off the need for shared situational awareness with maximizing individual intuition is a tough issue. The proper line between standoff and close-in combat on an illuminated battlespace is fuzzy at best.

Nevertheless, if the Grid is truly open, warfighters, singly or in teams, whether through their own efforts or through contracting, will be able to adapt it to their own needs. They can plug their own sensors and weapons into the Grid and find ways to mix their own information flows with global ones—they need not be organized from the top to do so.

The Grid should accelerate experimentation. If every unit has access to the same data flows, each can compete with others to make the best use of them (and with precision long-range weapons, many can engage any one target). The Grid should allow even military innovation at a pace known as "internet time." Indeed, there is no reason why allies, once plugged into the Grid, cannot compete with U.S. forces in coming up with new ideas, in ways hard to imagine with earlier technologies.

Technology Development

The act of creating the Grid will pose tough engineering problems, resolution of which will yield new technology. Because the basic technologies of the Grid already exist (assuming 10 years of expected advances in electronics), it is not science fiction. Accelerating some information technologies[48] would yield a better Grid faster—but which ones?

More power—processing speed, network throughput, memory capacity—always helps, but DOD will largely be a buyer, not a leader. Illumination and exploitation depend on the coordination of many small things, which means DOD needs improved ways to distribute power, rather than concentrate it. The importance of having more powerful personal systems (laptops and cellular phones) depends on how they are used. A twentyfold to fiftyfold improvement over today's systems, likely by 2015, may suffice if personal systems merely manage input to and output from the Grid. If personal systems process information off-line, there is no limit to what can be usefully wrung from technology.

Battlefield illumination requires the conversion of data to knowledge and thus a capability for image understanding, automatic target recognition, knowledge processing, text comprehension, and multisensory display. AI would help, but its progress has been slow. A more feasible approach may be to seek progress at both ends: reducing a data flood to a data stream and finding ways for people to work with successively larger streams. Automatic target recognition (ATR) may be best, but it may be enough if the Grid can take an image, eliminate most of it from further consideration, archive the rest for later analysis, and highlight what is essential for immediate human observation. Generating data and getting them into the right hands can be improved by knowing how to sift and sort efficiently, manipulating large data tables, thorough bookkeeping (tracking information and its changes), and fuzzy logic. The ability to translate human speech and text (especially with its author's help) into logically organized information and knowledge[49] could be used to sift through text, convert some of it into logic strings,[50] and help prepare and classify after-action reports. Displaying information is a matter of visualization, abstraction, semiotics, synthetic mapping superimposed on real maps, or ways to represent abstract data in two- and three-dimensional space to make intuitive sense.

Other technologies help a Grid's reliability, maintainability, flexibility, scalability, interoperability, and security. A Grid composed of interacting objects (nodes, sensors, weapons) is better managed as ecology than as machine; correctness is helpful, but so is a robust ability to adapt, protect, and expand itself easily. Security technologies may allow the Grid to diagnose and fix or dispose of compromised segments. Interoperability technologies may include methods a component can use to describe itself, test-and-probe techniques so that one system can assess the features of another, or ways to express goals, constraints, and tradeoffs. Whatever helps the Grid absorb innovation quickly, without reducing overall systems coherence, would yield a better Grid.

Many in the technology community see the RMA as validating their instinct to push technology vigorously. Left to themselves, however, the community will push technology everywhere. A clear vision of future warfare can focus efforts.[51]

Conclusions

The feasibility of building so large a Grid from the top down is untested, but problems with large systems suggest that bottom-up techniques be explored to increase both flexibility and robustness. Developing a Grid by incorporating legacy systems and engineering bottom-up features into its architecture should work better, but the process is not spontaneous.[52] A lexicon for communication among nodes needs to be developed, legacy systems disaggregation has to be negotiated, and central services must be planned. Roles for the services must be carefully negotiated so that they can become active and willing partners in the Grid's construction.

Notes

1. Some costs are difficult to pin down. Should the cost of adapting the data stream from a legacy sensor to the Grid's standards be included—especially if standards make sense even without a Grid?

2. See Tekla Perry,"In Search of the Future of Air Traffic Control," *IEEE Spectrum* 34, 8 (August 1997): 18-35. Hardware also played a role in the program's failure.

3. A dollop of dollars spent on connectivity can yield substantial improvements. The Army used off-the-shelf components and $6 million to jack together existing systems in order to cut the time to coordinate an attack on an enemy target from hours to seconds. Pat Cooper,"U.S. Army Officials say Data System Provides Rapid Attack," *Defense News,* February 20, 1995, 22. With comparable funding, the Air Force created a Combat Integration Capability that can locate a ballistic missile launch, warn troops of incoming missiles, and scramble fighters in less than 4 minutes. Frank Oliveri, "USAF Finds Low-Cost Key to Scud Fight," *Defense News,* November 27, 1995, 1. The Navy's Third Fleet assembled a real-time control center for a similarly low investment. DOD spent only $10.8 million (first release costs) for High Desert Tracon, a miniature version of the Federal Aviation Administration's new air traffic control system. Perry, 20-22. Unfortunately, getting these interoperability improvements to interoperate with one another and the Grid adds further costs.

4. The erstwhile arsenal ship was portrayed by the Navy as yet another fulcrum for interoperability. Pat Cooper and Robert Holzer, "U.S. Navy Sees Arsenal Ship as Catalyst for Interoperability," *Defense News,* September 9, 1996, 13.

5. Although the F-22 will not reach Air Force sqadrons before 2004, its avionics requirements were frozen in 1982.

6. Technology is being developed to capture the rationale for design decisions as they are reified in code. Good technology does not solve the whole problem; understanding the thought processes of another designer or programmer still takes work.

7. The Navy took 1,500 pages to spell out its requirements for computer-aided design workstations, computers that were highly standardized even in the late 1980s. Specifications for the Army's Reserve Component Automation System were roughly 10 times larger.

8. Many large service-initiated projects, such as the Army's TF XXI or Navy's acquisition of CAD systems, ought to be but are not born joint, in part because coordinating many constituencies within a single service is difficult enough without adding others from outside.

9. The Internet was designed so that researchers could share expensive equipment, such as mainframe computers, but its creators soon discovered that its main use was e-mail.

10. MITRE served as an integrator for the Army's TF XXI project; it developed the simulations and tests to validate overall functionality but wrote little code.

11. Peter Wegner, "Why Interaction Is More Important than Algorithms," *Communications of the ACM* 40 (May 5, 1997): 86, likened a sufficiently complex system to an elephant and observed: "Since a complete elephant cannot be specified, the focus shifts to specifying its parts and forms of behavior (such as its trunk or its mode of eating peanuts). Complete specification must be replaced by partial specification of the interfaces, views, and modes of use."

12. Microsoft has its own version of systems integration, according to Michael Cusumano and Richard Selby, *Microsoft Secrets* (New York: Free Press, 1995). The company relies on the synchronize-and-stabilize approach: the prototype finished code—the daily build—grows incrementally as a new list of features is added and integrated. Features are characterized as essential, important, and nice to have; projects meet their deadlines by shedding features in reverse order of priority. By defense standards, Microsoft projects are middle size. As of 1995, its most complex application, Excel®, ran just over a million lines of code, and its most complex product, Windows NT®, just under five million.

13. DOD may need to strengthen geospatial or security features. Maybe by the time the Grid is operational, commercial interfaces would permit the extensive user customization described in chapter 4.

14. Contrast the requirements of an algorithm that makes assumptions about the format, meaning, and precision of its input with one that assumes only that such meta-data will be stated in a standard way.

15. DOD tends to establish large programs to amalgamate specific subsystems into independent large-domain systems (intelligence, logistics, medical support), but cross-domain integration has value. Running theater simulations or testing alternative options for resupply may require using information from both intelligence and logistics databases. Data-discovery applications, which convert a user's queries into correct database formats, should not presume that the user knows into which domain a question falls.

16. Developing standards and writing tests for them remain costly and slow. The Open Systems Interconnection suite of data communications standards cost $1 to $2 billion to build—and data communications remain but a small subset of the standards the Grid needs. Counterpart Internet standards are less complex, but, at perhaps $100 million a year, not necessarily cheaper to develop (1,500 people attend binannual meetings of the Internet Engineering Task Force). Today's content standards ensure at most that well-formatted bytes can be passed and pigeonholed. Standards to handle software objects are limited to ensuring correct syntax: applications can call objects and use network services correctly. Semantic standards are needed to ensure that concepts can be transferred and mutually understood. DOD is working on a database dictionary, but the project has a long way to go, and many useful concepts do not lend themselves to databases. Although most of the DOD Common Operating Environment is necessary to Grid integration, it is certainly not sufficient.

17. In some cases, the software of a legacy system will need to be reworked to provide information that the Grid wants or whenever its data are insufficiently precise or too infrequently collected. Some legacy systems may be discarded if reworking them costs too much (just as some financial systems are retired because of the cost of fixing the year 2000 problem).

18. The advantage of sensors that can be externally queried and read passively (imagine a page that rewrites itself and reflects visible light) is that they are hard to detect and do not need large power sources. Whether they offer sufficient bandwidth is another issue.

19. By analogy, in object-oriented programming, code is written so that the actions a component can perform are listed in one place (a class definition) and thereby limited. Such code is more easily debugged than code in which commands to components are found everywhere in the program.

20. The Internet's simple network management protocol would probably be a good base if supplemented to accommodate the heterogeneity of defense systems (compared with LANs), higher equipment fault rates, and

real-time requirements.

21. Naked facts lack context. Nodes may need ways to ask and answer why this is so, why that matters, and so on. A polled sensor may ask what the poller is seeking (for example, the interrogator may not have access to sensor logs or know local conditions). An answer may change the request: Is it raining? *Why do you ask?* So I know whether to wear a jacket. *We are not going anywhere.* Don't we need groceries? *No, I picked them up yesterday.* Or, the question "Is it raining?" may be posed because plants may need watering.

22. Primary sources can be killed, cut off, compromised, made otherwise unreliable, or just unsatisfactory. Requesters will need to know second-best ways to acquire knowledge, which will vary by task: less responsive, less trustworthy, less detailed, collecting similar but not identical data, or know a broker who can point to second-best sources.

23. The logistics community, in particular, has wrestled with this problem for eons—one reason that the director for logistics for the JCS has been given such a key role in C^4ISR integration—but these problems also arise with battlespace illumination. An image of something sticking up could be a Scud launcher or a telephone pole. A database of phone lines and poles might help differentiate them, but it may be only 99 percent complete (leaving far more uncounted poles then Scud launchers) or ignore information about the pole's height and thickness that may help distinguish one from the other.

24. A program from Lockheed (Simulation Assessment Validation Environment) knits together CAD software, modeling programs, scheduling and work-flow simulations, and risk analysis algorithms (see William Scott, "Integrated Software to Cut JSF, F-22 Costs," *Aviation Week and Space Technology,* May 13, 1996, 64-65.

25. For instance, a form used to plan projects, can, with minor modification, help schedule project-related conferences and, with other minor modification, help project expenses and, with yet other minor modification, help forecast requirements for new hires. The more constituencies that need the information, the greater the burden on the project planer.

26. Doug Lenat created CyC, a million-fact common-sense knowledge base, by using one unified way to organize knowledge (ontology), one vocabulary of relationships, and one processing engine. Even so, CyC runs slowly. Were the Grid to use a single way of stating knowledge and a single way of asking about it, it would still be necessary to separate knowledge by domain (e.g., guerilla tactics, street crime) and then find experts in each.

27. But does pointing to a large brown table convey pointing, large, brown, table, or the need to look?

28. Even established allies cannot automatically be expected to follow U.S. standards, formal or de facto, but international standards are often slow in coming and unwieldy in practice.

29. As an example, the Internet's Domain Name Service, which translates common names into address bytecodes, is an integrated mechanism, but the translation is actually performed in numerous country-specific and domain-specific servers.

30. With chips, fiber, and disk drives cheaper by the day, there may be no scarce resources and thus nothing to allocate. So far, information demands and technology have risen in tandem, and sometimes improving everything shifts but does not fix problems. For example, if both a computer's processor speed and its disk capacity are doubled, searching through its hard memory takes just as long. Without management, legacy systems (particularly those hard-wired into long-lived weapons systems) may be flooded. Poorly written software or information warfare may generate unlimited traffic.

31. A socket is the way a node interacts with a service; if the service is removed, the socket can be discarded, which eases node management.

32. The DOD C[4]ISR Integration Support Activity, *C[4]ISR Architecture Framework: Version 1.0*, of June 7, 1996.

33. The Grid needs a good mix of top-down and bottom-up programming. In a top-down approach, each task would result in program statements inserted into every supporting node. Nodes that support many tasks would have to host code for each single task, a need that could lead to overly complex software and risk unanticipated interactions among code elements. Alternatively, each node would be engineered for only one task, leaving it inflexible in meeting new requirements. A bottom-up approach would translate tasks (below some level) into requests or statements for each node and written in a standard lexicon. Every node would come equipped with code to let it respond to standard requests, so that every new task would specify what but not necessarily how.

34. Formal allies clearly qualify. Rogue states do not. Potential powers, such as Russia, Ukraine, China, India, and Indonesia, could qualify if they renounced force (including terrorism) to settle international disputes and did not use the Grid's information to violate human rights.

35. Examples include security authentication, procedures for number crunching, formats to display data, alert lists, logic algorithms, software for pattern recognition, event-based learning, and intelligent agents.

36. A Grid could host private value-added-network data and services on top of core data and services. Typically, defense contractors supply these services to DOD for development costs (plus profit) and try to make big money from exports. DOD interests lie in making the basic package as attractive as possible, but that may require persuading contractors to make their profits, not by selling software, but on adapting generic software to specific customers, serving their individual needs, and providing consultation.

37. Establishing and demonstrating a long lead over probable challengers may dissuade them from competing in the first place. See Seymour Goodman, "War, Information Technologies, and International Asymmetries," *Communications of the ACM* 39 (December 12, 1996): 11-15.

38. Yet opening the Grid means accepting its use for purposes that the U.S. may not condone, much less authorize, and finding ways to frustrate others from copying what it sees (especially the standards that embody what U.S. firms know about how to integrate systems).

39. James Blaker, private communication. See also William Owens and Joseph Nye, "America's Information Edge," *Foreign Affairs* 75, 2 (March-April 1996): 20-36.

40. Fear of China is currently the major but not sole impetus for arms acquisition. Steve Glain, "Fearing China's Plans and a U.S. Departure, Asians Rebuild Forces," *The Wall Street Journal*, November 13, 1997, A1.

41. William Sweet, "Better Networks for Test Ban Monitoring," *IEEE Spectrum* 33, 2 (February 1996), 26. A key part of the system is provided by the Group of Scientific Experts Technical Test, proposed by the Swedes and supported by DARPA's Center for Monitoring Research.

42. In a limited war, the goal is not annihilation but settlement. One party could use the open Grid to demonstrate what it can see (thus, what it can hit) and so negotiate the surrender or withdrawal of the other. Simulations, were they more credible and transparent than now possible, could show what one side could do to the other in a particular scenario. Signalling could be used locally, so that particular positions could be settled without their fate being determined by blood. A military that wanted to find an honorable way to withdraw from an untenable position could use information from the Grid to argue before its political masters that it had no good alternative.

Conversely, a military (particularly the underdog's) could publicly yank its Grid connections as a refusal to enter into games (much as diplomats are withdrawn immediately prior to the outbreak of hostilities). In private, a few circuits could stay up. Each side could have patrons, themselves interlinked. Neither would wish itself voluntarily cut off from the global network. Each

could require information from the same providers, whether sophisticated, multinational consultants or local service vendors. So long as a mutual conduit exists, the possibility of its use will exist also.

43. When information is 10 percent of combat force, it is the tail; when it is 90 percent, it is the dog, and information can be privatized more easily than the use of organized force can be. Contractors, whose role was almost nonexistent during the Korean War, were modestly important in the Vietnam conflict, critical in the Gulf War (JSTARS needed Grumman employees on board), and essential to the Haiti operation. Whether Croatia could have recaptured Krajina from Serb forces in 1995 without the help of Military Professional Resources International, Inc., is not clear. The line between military and civilian information has become fuzzy. Raytheon, which developed the System for the Vigilance of the Amazon, an environmental surveillance network, has offered something similar to support peacekeeping in the Golan and Bosnia.

44. By starting from the future and working back, designers can leave a placeholder for features technology allows or that growth dictates. Consider how many times Army's Force XXI project may need to be rewritten in the next few years. When bandwidth to the field rises (from the current 9,600 bps), limitations on querying or logging onto the very capable systems found in battalion tactical operation centers will seem pointless. Getting close air support from the Air Force requires the Army to extend its tactical internet across service lines. As the Army realizes the intelligence advantages of internetted sensors, it will want to digitize its platforms, which means hosting a wide range of data flows from platform sensors and to platform controls through the bandwidth-limited Appliqué. Finally, meeting the challenge of information warfare could require an intensive security layer atop extant software.

45. A software version of the Official Airline Guide tells users about flights. It rests upon a database (flight number, carrier, city pair, equipment, cost, etc.) inaccessible except through the application. Ordinarily, the application gives travelers what they need, but without direct access to the data-base, one cannot ask new questions: where does the flight from Cleveland to Chicago originate, what airports handle Boeing 747s? The ability to ask new questions of data leads to innovations in perception.

46. Report of the National Defense Panel, *Transforming Defense: National Security in the 21st Century* (December 1, 1997), 68-70, and www.dtic.mil/ndp.

47. Do experiments need to use world-scale forces to be valid? In late 1997, the Army Chief of Staff advocated a joint experimental force of 50,000; the Joint Staff's Vanguard Force envisioned 300,000. The need for scale is not

clear. For peace operations and low-intensity combat (and thanks to networking), the locus of effective military action is going to be at the squad and company level on the ground and the lone plane or squadron in the air. As high-intensity combat becomes hide-and-seek warfare, massed militaries in broad movements will be less important than the prosecution of individual enemy mistakes using minimal force packages.

48. The Grid can use better technologies for, say, sensors (including nanotechnologies such as microeletromechanical systems, radioelectronics), compact power, and smart weaponry.

49. Semantic processing works better in microworlds. The military domain seems to be in between, in that its training standardizes action, including speech acts. Error rates on a restricted vocabulary Naval Battle Management corpora are a tenth of normal conversational speech. Even if military speech were sufficiently routinized to be recognized, can it can be processed as symbolic knowledge?

50. Jim Cowie and Wendy Lenhert, "Extracting Information," *Communications of the ACM* 39, (January 1, 1996): 80-91, have argued that today's technology is good enough to allow users to extract certain types of information from textual material.

51. Vision helps, but no vision should have more than a limited influence on overall DOD information technology research agenda for the following reasons:

- Information technologies that improve production tools (e.g., CAD, testing, or training) logistics characteristics may be worthwhile regardless of scenario
- Visions may err. A military consumed by peace operations or WMD countermeasures may need technologies different from those called for by standoff warfare, and really good armor or ways to engage swarms of weapons may prolong the era of platforms).
- Serendipity matters.

52. Robert Metcalfe, the inventor of the Ethernet, has argued that a system as complex as the Internet needs to be managed, engineered, and financed as a network of computers, rather than as an unfathomable biological organism; see George Gilder, "Feasting on the Giant Peach," *ASAP Forbes,* August 16, 1996, 86.

6.
Conclusions

Successively deeper infusions of information technology into DOD military equipment would, in and of itself, help it fight better, but information technology can also transform the capabilities of the U.S. military in two fundamental ways:

- Illuminating the battlespace will permit DOD to see and therefore defeat foes by striking from standoff range or by supporting local warfighters with information. Thus DOD can cope with foes nastier than today's canonical opponents.
- A sufficiently adaptive Grid may help warfighters see patterns of conflict in complex and chaotic situations enabling the DOD to cope with messier situations better.

To see well, DOD must have a vision for its Grid. Otherwise, what it calls the Grid will be merely the clutter of point solutions to point problems, incapable of integration and inflexible against a foe with a talent for the unexpected. Let bits be bits. If they are accessible and the tools for their exploitation exist, knowledge can be drawn from them. An adaptive Grid is more difficult to build and, in many ways, control (although not necessarily harder to manage). But it is an important ideal with these features:

- *Input.* Complex sensors would be supplemented with a mesh of distributed commercial-grade sensors (and some bistatic ones). Automatic coordination of sensors would be the rule, especially for ground sensors or cheap UAVs.
- *Connectivity.* Nodes would not only transfer messages but, in many cases, also understand them. Bandwidth to the field would suffice for visual exchange and whiteboarding. Messages would

be routed on the basis of such criteria as content (rather than only subject) and user context (not just identity) to support automatic event-driven notification. Allies would enjoy broad access to the Grid.

- *Processing.* Facts would affect estimates based on criteria and rules that can be developed as needed. Particular sensor readings, events, and agent-initiated actions could spur further data processing. To respond to complex questions, the Grid could summon experts and present them with complex tableaux for evaluation.
- *Geoprocessing.* The link among image acquisition, object identification, and object location would be automatic or nearly so. Broadcasting data would allow weapons to track moving targets by reference to location.
- *Integrity.* Flexibility in design and sufficient systems abstraction, among other tools, would help users merge disparate systems in nearly real time. Any unexpected condition that generates incorrect behavior would be scrutinized. New capabilities, once resident and cleared, could announce themselves.
- *Output.* Users could manipulate data flow and presentation to raise their intuitive understanding of what they were looking at. They could use many tools to search for information.

Because great change without great challenge is perilous, the argument for the Grid must be explicit.[1] Technology is not the issue;[2] the United States will always lead with its strongest suit. The issue is *what* technology *where*. Platforms are starting to look like the mainframe computers of war,[3] at once too big (compared with individual commercial-grade sensors and weapons) and too small (compared with the knowledge base of a fully networked establishment). Monolithic information systems are both too complex and too narrow. When material purchased between the 1960s and the 1980s wears out, decisions on how to recapitalize the military, if made in the context of today's force structure, may ensure that tomorrow's military will have the look and feel of yesterday's.

DOD can ignore what technology is saying; today's adversaries seem even more blind. But it is asking a lot of history that they remain blind forever. Some day, others, not necessarily friendly others, will see the light. It would be best if the light they see is ours.

Notes

1. Germany's *Blitzkrieg*, France's *Levée en Masse*, and the U.S. Navy–USMC carrier operations and amphibious warfare all suggest that an RMA needs not only technology but also a pressing problem (avoiding trench warfare, taking on every *ancien regime* at once, and operating across the Pacific, respectively). This theme runs through several essays in Williamson Murray and Allan Millett, *Military Innovation in the Interwar Period* (Cambridge, England: Cambridge University Press, 1996): Geoffrey Till, "Adopting the Aircraft Carrier: the British, American, and Japanese Case Studies," 22: "The ability to predict who [the British] would be fighting and when was especially uncertain and this shortcoming had a direct bearing on the capabilities the Royal Navy needed to produce. Having more specific incentives, the Americans and Japanese were better placed . . . [to] create a climate more conducive to innovation." Alan Beyerchen's "From Radio to Radar: Interwar Military Adaptation to Technological Change in Germany, the United Kingdom, and the United States," 298: "Although technical developments ran roughly parallel in time in Germany, Britain, and the United States, the British jumped ahead operationally and technologically because they perceived a need to adapt to a situation they had not caused and could not control. The Germans thought that they could control events and the Americans saw no need to."

2. RMA advocates argue that it promotes more capability for *less* money. See James Blaker, *Understanding the Revolution in Military Affairs: A Guide to America's 21st Century Defense* (Washington: Progressive Policy Institute, January 1997), 20.

3. Those who recall what nuclear strategists wrote—for example, Lawrence Freedman, *The Evolution of Nuclear Strategy* (New York: St. Martin's, 1981, 1989) may be forgiven for remembering earlier predictions that conventional forces would be obsolete in the face of nuclear weapons. Complete battle groups were expected to be vaporized by any H-bomb within 10 kilometers. It was believed a nation's airfields would quickly become useless after being hit by an initial nuclear strike. Armies trained to concentrate force would find their concentrations excellent targets for mass annihilation and would need to disperse to survive (hence the ill-fated Pentomic division of the late 1950s). Conventional forces are still here—so

what happened to yesterday's future? Korea and Vietnam showed that U.S. forces and arms need to wage lesser wars and compete with forces equipped with Soviet-supplied arms in scenarios lacking credible nuclear options. As Bernard Brodie was the first to note, it is difficult to conceive of any military operations with usable nuclear options. From roughly 1960 on, the services returned to contemplating conventional defense against the Soviets because that could be sustained without all-out nuclear warfare, preferably without any nuclear weapons whatsoever. In contrast to nuclear weapons, the Grid could be eminently usable.

Acronyms

ABIS	advanced battlespace information system
ACTD	advanced concept technology demonstrations
AI	artificial intelligence
ATACMS	army tactical missile system
ATM	asynchronous transfer mode
ATO	air tasking order
ATR	automatic target recognition
AWACS	airborne warning and control system
BADD	battlefield awareness and data dissemination
bps	bits per second
C^4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CAD	computer-aided design
COP	common operational picture
DARPA	Defense Advanced Projects Research Agency
DBS	direct broadcast satellite
DGPS	differential GPS
DISA	Defense Information Systems Agency
DOD	Department of Defense
FOG-M	fiber-optic guided missile
GCCS	global command and control system
GLONASS	global navigation satellite system
GPS	global positioning system
INS	inertial navigational system
IR	infrared
JDAM	joint direct attack munition
JSTARS	joint surveillance, target attack radar system
LAN	local area network
LEO	low-earth orbit
MEMS	micro-electromechanical system
MTW	major theater war
NASA	National Aeronautics and Space Administration

NATO	North Atlantic Treaty Organization
PGM	precision-guided munitions
RF	radio frequency
RMA	revolution in military affairs
SAR	synthetic aperture radar
TADIL	tactical digital information link
TF	task force
UAV	unmanned aerial vehicle
USMC	U.S. Marine Corps
WMD	weapons of mass destruction
WWW	World Wide Web

About the Author

Martin C. Libicki is a senior policy analyst with The RAND Corporation in Washington. Previously, he was a senior fellow at the Institute for National Strategic Studies, National Defense University, where he specialized in the application of information technologies to national security issues, information warfare, information technology standards, and the revolution in military affairs.

Dr. Libicki is the author of *What Is Information Warfare?*, *Standards: The Rough Road to the Common Byte*, and *The Mesh and the Net*, and co-editor *of Dominant Battlespace Knowledge*. Most recently, he co-authored *Mind the Gap: Promoting a Transatlantic Revolution in Military Affairs* (Washington: National Defense University Press, 1999).

McNair Papers

The McNair Papers are published at Fort Lesley J. McNair, home of the National Defense University. An Army installation since 1794, the post was named in honor of Lieutenant General Lesley James McNair in 1948. McNair, known as the "Educator of the Army" and trainer of some three million troops, was about to take command of Allied Ground Forces in Europe under General Eisenhower, when he was killed in combat in Normandy on July 25, 1944.

The following is a complete list of McNair Papers. For information on availability of specific titles, contact the NDU Press.

1. Joseph P. Lorenz, *Egypt and the New Arab Coalition*, February 1989.
2. John E. Endicott, *Grand Strategy and the Pacific Region*, May 1989.
3. Eugene V. Rostow, *President, Prime Minister, or Constitutional Monarch?* October 1989.
4. Howard G. DeWolf, *SDI and Arms Control,* November 1989.
5. Martin C. Libicki, *What Makes Industries Strategic,* November 1989.
6. Melvin A. Goodman, *Gorbachev and Soviet Policy in the Third World,* February 1990.
7. John Van Oudenaren, "The Tradition of Change in Soviet Foreign Policy," and Francis Conte, "Two Schools of Soviet Diplomacy," in *Understanding Soviet Foreign Policy,* April 1990.
8. Max G. Manwaring and Court Prisk, *A Strategic View of Insurgencies: Insights from El Salvador,* May 1990.
9. Steven R. Linke, *Managing Crises in Defense Industry: The PEPCON and Avtex Cases,* June 1990.
10. Christine M. Helms, *Arabism and Islam: Stateless Nations and Nationless States,* September 1990.
11. Ralph A. Cossa, *Iran: Soviet Interests, US Concerns,* July 1990.
12. Ewan Jamieson, *Friend or Ally? A Question for New Zealand,* May 1991.
13. Richard J. Dunn III, *From Gettysburg to the Gulf and Beyond: Coping with Revolutionary Technological Change in Land Warfare,* March 1992.
14. Ted Greenwood, *U.S. and NATO Force Structure and Military Operations in the Mediterranean,* June 1993.
15. Oscar W. Clyatt, Jr., *Bulgaria's Quest for Security After the Cold War*, February 1993.
16. William C. Bodie, *Moscow's "Near Abroad": Security Policy in Post-Soviet Europe*, June 1993.

17. William H. Lewis (ed.), *Military Implications of United Nations Peacekeeping Operations*, June 1993.
18. Sterling D. Sessions and Carl R. Jones, *Interoperability: A Desert Storm Case Study*, July 1993.
19. Eugene V. Rostow, *Should Article 43 of the United Nations Charter Be Raised From the Dead?* July 1993
20. William T. Johnsen and Thomas Durell-Young; Jeffrey Simon; Daniel N. Nelson; William C. Bodie, and James McCarthy, *European Security Toward the Year 2000,* August 1993.
21. Edwin R. Carlisle, ed., *Developing Battlefield Technologies in the 1990s,* August 1993.
22. Patrick Clawson, *How Has Saddam Hussein Survived? Economic Sanctions, 1990–93,* August 1993.
23. Jeffrey Simon, *Czechoslovakia's "Velvet Divorce," Visegrad Cohesion, and European Fault Lines,* October 1993.
24. Eugene V. Rostow, *The Future of Palestine,* November 1993.
25. William H. Lewis, John Mackinlay, John G. Ruggie, and Sir Brian Urquhart, *Peacekeeping: The Way Ahead?* November 1993.
26. Edward Marks and William Lewis, *Triage for Failing States,* January 1994.
27. Gregory D. Foster, *In Search of a Post-Cold War Security Structure*, February 1994.
28. Martin C. Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*, March 1994.
29. Patrick Clawson, ed., *Iran's Strategic Intentions and Capabilities*, April 1994.
30. James W. Morrison, *Vladimir Zhirinovskiy: An Assessment of a Russian Ultra-Nationalist*, April 1994.
31. Patrick M. Cronin and Michael J. Green, *Redefining the U.S.-Japan Alliance: Tokyo's National Defense Program*, November 1994.
32. Scott W. Conrad, *Moving the Force:* Desert Storm *and Beyond*, December 1994.
33. John N. Petrie, *American Neutrality in the 20th Century: The Impossible Dream*, January 1995.
34. James H. Brusstar and Ellen Jones, *The Russian Military's Role in Politics*, January 1995.
35. S. Nelson Drew, *NATO from Berlin to Bosnia: Trans-Atlantic Security in Transition*, January 1995.
36. Karl W. Eikenberry, *Explaining and Influencing Chinese Arms Transfers*, February 1995.
37. William W. Mendel and David G. Bradford, *Interagency Cooperation: A Regional Model for Overseas Operations*, March 1995.

38. Robbin Laird, *French Security Policy in Transition: Dynamics of Continuity and Change*, March 1995.
39. Jeffrey Simon, *Central European Civil-Military Relations and NATO Expansion*, April 1995.
40. James W. Morrison, *NATO Expansion and Alternative Future Security Alignments in Europe*, April 1995.
41. Barry R. Schneider, *Radical Responses to Radical Regimes: Evaluating Preemptive Counter-Proliferation*, May 1995.
42. John Jaworsky, *Ukraine: Stability and Instability*, July 1995.
43. Ronald Tiersky, *The Mitterrand Legacy and the Future of French Security Policy*, August 1995.
44. John A. Cope, *International Military Education and Training: An Assessment*, October 1995.
45. Elli Lieberman, *Deterrence Theory: Success or Failure in Arab-Israeli Wars?* October 1995.
46. Stanley R. Sloan, *NATO's Future: Beyond Collective Defense*, December 1995.
47. M. E. Ahrari, *The New Great Game in Muslim Central Asia*, January 1996.
48. Mark J. Roberts, *Khomeini's Incorporation of the Iranian Miilitary*, January 1996.
49. Steven Philip Kramer and Irene Kyriakopoulos, *Trouble in Paradise? Europe in the 21st Century*, March 1996.
50. Alan L. Gropman, *Mobilizing U.S. Industry in World War II: Myth and Reality*, August 1996.
51. Ralph A. Cossa, *The Major Powers in Northeast Asian Security*, September 1996.
52. Barry D. Watts, *Clausewitzian Friction and Future War*, October 1996.
53. Donna Lee Van Cott, *Defiant Again: Indigenous Peoples and Latin American Security*, October 1996.
54. Ivelaw L. Griffith, *Caribbean Security on the Eve of the 21st Century*, September 1996.
55. Roman Popadiuk, *American-Ukrainian Nuclear Relations*, October 1996.
56. Simon V. Mayall, *Turkey: Thwarted Ambition*, January 1997.
57. David L. Johnson, *Modern U.S. Civil-Military Relations: Wielding the Terrible Swift Sword*, July 1997.
58. William H. Lewis and Edward Marks, *Searching for Partners: Regional Organizations and Peace Operations*, June 1998.
59. David C. Gompert, *Right Makes Might: Freedom and Power in the Information Age*, May 1998.
60. Robbin F. Laird and Holger H. Mey, *The Revolution in Military Affairs: Allied Perspectives*, April 1999.

Electronic Publications

The Institute for National Strategic Studies (INSS) provides a growing list of publications on the World Wide Web including:

NDU Press Books—works by statesmen, scholars, specialists, and students in the fields of strategic studies, defense policy, and military affairs (all volumes since 1996 as well as selected back titles)

Strategic Assessment—a comprehensive illustrated annual report prepared since 1995 on major strategic issues of the day (all editions)

Strategic Forums—four-page briefs on a wide range of international security issues written by leading defense analysts (more than 160 titles)

McNair Papers—monographs on key foreign and defense policy topics (all papers since 1996 and selected back titles)

http://www.ndu.edu/ndu/inss/press/nduphp.html

Joint Force Quarterly (JFQ)—a professional military journal published for the Chairman, Joint Chiefs of Staff, to promote understanding of the integrated employment of land, sea, air, space, and special operations forces. *JFQ* focuses on joint doctrine, coalition warfare, contingency planning, combat operations conducted by unified commands, and joint force development (all issues).

http://www.dtic.mil/doctrine/jel

An on-line catalog of publications—both electronic and printed—will be available later this year. In the meantime, explore our home page for titles published by INSS as well as other components of National Defense University:

http://www.ndu.edu

INSTITUTE FOR NATIONAL STRATEGIC STUDIES
NATIONAL DEFENSE UNIVERSITY